Guidelines for Cybersecurity Education Campaigns

by

Rayne Reid

Thesis
Submitted in fulfilment
of the requirements
for the degree

Doctor of Philosophy
in
Information Technology
in the
Faculty of Engineering, the Built Environment and
Information Technology
of the
Nelson Mandela University

Promoter: Prof Johan Van Niekerk

August 2017
Declaration

I, Rayne Reid (s208045820), hereby declare that:

- The work in this thesis is my own work.
- All sources used or referred to have been documented and recognized.
- This thesis has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognized educational institute.

Rayne Reid
Abstract

In our technology- and information-infused world, cyberspace is an integral part of modern-day society. As the number of active cyberspace users increases, so too does the chances of a cyber threat finding a vulnerable target increase. All cyber users who are exposed to cyber risks need to be educated about cyber security.

Human beings play a key role in the implementation and governing of an entire cybersecurity and cybersafety solution. The effectiveness of any cybersecurity and cybersafety solutions in a societal or individual context is dependent on the human beings involved in the process. If these human beings are either unaware or not knowledgeable about their roles in the security solution they become the weak link in these cybersecurity solutions. It is essential that all users be educated to combat any threats.

Children are a particularly vulnerable subgroup within society. They are digital natives and make use of ICT, and online services with increasing frequency, but this does not mean they are knowledgeable about or behaving securely in their cyber activities. Children will be exposed to cyberspace throughout their lifetimes. Therefore, cybersecurity and cybersafety should be taught to children as a life-skill.

There is a lack of well-known, comprehensive cybersecurity and cybersafety educational campaigns which target school children. Most existing information security and cybersecurity education campaigns limit their scope. Literature reports mainly on education campaigns focused on primary businesses, government agencies and tertiary education institutions. Additionally, most guidance for the design and implementation of security and safety campaigns: are for an organisational context, only target organisational users, and mostly provide high-level design recommendations.

This thesis addressed the lack of guidance for designing and implementing cybersecurity and cybersafety educational campaigns suited to school learners as a target audience. The thesis aimed to offer guidance for designing and implementing education campaigns that educate school learners about cybersecurity and cybersafety. This was done through the implementation of an action research process over a five-year period. The action research process involved cybersecurity and cybersafety educational interventions at multiple schools. A total of 18 actionable guidelines were derived from this research to guide the design and implementation of cybersecurity and cybersafety education campaigns which aim to educate school children.
**Acknowledgement**

I am very grateful that I have had the opportunity to undertake my Doctoral studies. I feel blessed to have received so much support and guidance throughout this process. I would like to offer my sincere thanks to the following people and institutions:

My research promoter, Prof Johan van Niekerk, whose knowledge and, valuable and constructive suggestions greatly aided the planning and progress of this research work. His patience, and willingness to give his time so generously has been very much appreciated.

My financial benefactors, National Research Foundation and Vodacom/NMMU, whose financial support enabled me to continue with my education.

- *The financial assistance of the National Research Foundation (NRF Innovation Doctoral Scholarship) towards this research is hereby acknowledged. Opinions expressed, and conclusions arrived at, are those of the author and are not necessarily to be attributed to the NRF.*

- *The financial assistance by the Vodacom/NMMU scholarship towards this research is hereby acknowledged. Opinions expressed, and conclusions arrived at are those of the author and are not necessarily to be attributed to the sponsors.*

My parents, Ronel and Darryl (in heaven), and my siblings, Christopher and Hannah, whose support, encouragement and understanding helped me to progress even in the most challenging moments of my studies.
# Table of Contents

1 Introduction ............................................................................................................. 1  
  1.1 Background ........................................................................................................ 2  
  1.2 Fields of Study .................................................................................................... 4  
  1.3 Problem Statement ............................................................................................. 4  
  1.4 Thesis Statement ................................................................................................ 5  
  1.5 Delineation ......................................................................................................... 5  
  1.6 Research Questions ............................................................................................. 6  
  1.7 Research Objectives ............................................................................................ 7  
  1.8 Research Methodology ....................................................................................... 8  
  1.9 Structure of the thesis ......................................................................................... 8  

2 Information Security and Cybersecurity ................................................................. 13  
  2.1 Introduction ......................................................................................................... 14  
  2.2 Context of the Study ........................................................................................... 14  
  2.3 Information Security and Cybersecurity ............................................................. 20  
    2.3.1 Information Security ....................................................................................... 22  
    2.3.2 Cybersecurity ................................................................................................ 24  
  2.4 The Human Factor of Cybersecurity .................................................................. 26  
  2.5 Information Security Culture to Cybersecurity Culture ...................................... 28  
    2.5.1 Information Security Culture ......................................................................... 28  
    2.5.2 Considerations for a Cybersecurity Culture .................................................. 31  
    2.5.3 How to Foster a Culture ................................................................................ 35  
  2.6 The Scope of this Research .................................................................................. 39  
  2.7 Conclusion .......................................................................................................... 41  

3 Information Security and Cybersecurity Education ................................................. 42  
  3.1 Introduction ......................................................................................................... 43  
  3.2 Scope of Review .................................................................................................. 45
3.3 Comprehensive Review of existing information security and cybersecurity educational literature ........................................46

3.3.1 Standards ..................................................................................................................46

3.3.2 National Imperatives ...............................................................................................54

3.3.3 Curriculum Guidelines ..........................................................................................57

3.3.4 Related Research ...................................................................................................57

3.4 Overview of literature findings ..................................................................................101

3.5 Conclusion ................................................................................................................106

4 Methodology and Research Process ............................................................................107

4.1 Introduction ................................................................................................................108

4.2 Research Design ........................................................................................................109

4.2.1 Research Philosophy ............................................................................................110

4.2.2 Research Approach and Data choice ......................................................................113

4.2.3 Research Strategy ..................................................................................................114

4.2.4 Methodological Choice ........................................................................................118

4.2.5 Time Horizon .........................................................................................................119

4.2.6 Techniques and Procedures ..................................................................................120

4.2.7 Overview of Choices Made for this thesis ............................................................120

4.3 Research Process ........................................................................................................121

4.4 Research Design Considerations ..............................................................................125

4.5 Conclusion ................................................................................................................125

5 Theoretical Basis used in Action Research Interventions ...........................................127

5.1 Introduction ................................................................................................................128

5.2 Brain-compatible Education .....................................................................................130

5.2.1 Brain-compatible Education Principles ...............................................................133

5.2.2 A learning experience should be as multifaceted as possible, catering for as many learning styles as possible and providing as many opportunities for each learner to develop as far as possible .........................................................135
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Introduction</td>
<td>250</td>
</tr>
<tr>
<td>9.2</td>
<td>Problem Identification</td>
<td>250</td>
</tr>
<tr>
<td>9.2.1</td>
<td>Establish a more formalised education approach with supporting materials</td>
<td>251</td>
</tr>
<tr>
<td>9.2.2</td>
<td>Examine the effect of method(s) used to gain achieve school participation and gain the learners attention</td>
<td>252</td>
</tr>
<tr>
<td>9.2.3</td>
<td>Re-evaluate the effectiveness of the cybersecurity education game</td>
<td>253</td>
</tr>
<tr>
<td>9.2.4</td>
<td>Increase the relevance and relatability of the campaign and its content for the learners</td>
<td>253</td>
</tr>
<tr>
<td>9.2.5</td>
<td>Determine whether a correlation exists between campaign’s content emphasis and the content choices learners depict in posters</td>
<td>254</td>
</tr>
<tr>
<td>9.3</td>
<td>Action planning</td>
<td>254</td>
</tr>
<tr>
<td>9.3.1</td>
<td>Target audience</td>
<td>255</td>
</tr>
<tr>
<td>9.3.2</td>
<td>The Educational Campaign</td>
<td>256</td>
</tr>
<tr>
<td>9.3.3</td>
<td>The Competition</td>
<td>262</td>
</tr>
<tr>
<td>9.3.4</td>
<td>Measurements for use in the analysis of the campaign</td>
<td>264</td>
</tr>
<tr>
<td>9.4</td>
<td>Implementation</td>
<td>266</td>
</tr>
<tr>
<td>9.4.1</td>
<td>School A</td>
<td>267</td>
</tr>
<tr>
<td>9.4.2</td>
<td>Other Schools</td>
<td>267</td>
</tr>
<tr>
<td>9.5</td>
<td>Results and Evaluation</td>
<td>269</td>
</tr>
<tr>
<td>9.5.1</td>
<td>School A</td>
<td>270</td>
</tr>
<tr>
<td>9.5.2</td>
<td>Other Schools</td>
<td>276</td>
</tr>
<tr>
<td>9.5.3</td>
<td>General Results</td>
<td>292</td>
</tr>
<tr>
<td>9.6</td>
<td>Reflections</td>
<td>304</td>
</tr>
<tr>
<td>9.6.1</td>
<td>Establish a more formalised education approach with supporting materials</td>
<td>305</td>
</tr>
<tr>
<td>9.6.2</td>
<td>Examine the effect of method(s) used to achieve school participation and gain learners’ attention</td>
<td>308</td>
</tr>
<tr>
<td>9.6.3</td>
<td>Re-evaluate the effectiveness of the cybersecurity education game</td>
<td>310</td>
</tr>
</tbody>
</table>
9.6.4 Increase the relevance and relatability of the campaign and its content for the learners .................................................................311

9.6.5 Examine whether a correlation exists between campaign’s content emphasis and the content choices depicted in posters .........................313

9.7 Conclusion .................................................................................................314

10 Action Research Cycle 3: 2014 ...................................................................315

10.1 Introduction ...............................................................................................316

10.2 Problem Identification .............................................................................316

10.2.1 Establish a more formalised education approach with supporting materials ...317

10.2.2 Examine the effect of method(s) used to gain school participation and gain learners’ attention .................................................................318

10.2.3 Increase the relevance of the campaign and its content for learners ........319

10.2.4 Adapt the campaign to make it more adaptable .......................................319

10.3 Action planning ..........................................................................................320

10.3.1 Target audience ......................................................................................321

10.3.2 The Educational Campaign ..................................................................322

10.3.3 The Competition ....................................................................................333

10.3.4 Measurements for use in the analysis of the campaign .........................334

10.4 Implementation .........................................................................................336

10.4.1 School A ..................................................................................................336

10.4.2 Other Schools ..........................................................................................337

10.5 Results and Evaluation ............................................................................339

10.5.1 School A ..................................................................................................340

10.5.2 Other Schools ..........................................................................................345

10.5.3 General Results .......................................................................................354

10.6 Reflections .................................................................................................359

10.6.1 Establish a more formalised education approach with supporting materials ...359
10.6.2 Examine the effect of method(s) used to achieve school participation and gain learners’ attention .................................................................361
10.6.3 Increase the relevance of the campaign and its content for the learners........362
10.6.4 Adapt the campaign to be more manageable ..................................................362
10.7 Conclusion ........................................................................................................363

11 Action Research Cycle 4: 2015 .........................................................................365
11.1 Cycle 4: 2015 ..................................................................................................366
11.2 Problem Identification ....................................................................................366
11.2.1 The continued need for a formalised education approach, including formalised education material and the involvement of educators ...........367
11.2.2 The need to determine whether the audience is interpreting the campaign message(s) as the they are intended to be interpreted..............367
11.3 Action planning ...............................................................................................368
11.3.1 Target audience ............................................................................................369
11.3.2 The Educational Campaign ..........................................................................369
11.3.3 The Competition ..........................................................................................372
11.3.4 Measurements for use in the analysis of the campaign ...............................373
11.4 Implementation ................................................................................................378
11.4.1 School A ......................................................................................................379
11.4.2 Other Schools ..............................................................................................379
11.5 Results and Evaluation ....................................................................................381
11.5.1 School A ......................................................................................................382
11.5.2 Other Schools ..............................................................................................388
11.5.3 General Results ..........................................................................................397
11.6 Reflections ........................................................................................................403
11.6.1 The continued need for a formalised education approach, including formalised education material and the involvement of educators ........403
11.6.2 The need to determine whether the audience is interpreting campaign message(s) as intended..............................................................404

11.7 Conclusion ...................................................................................................................405

12 Conclusion ..........................................................................................................................406

12.1 Introduction ......................................................................................................................407

12.2 Summary of Lessons Learnt..............................................................................................408

12.3 Summary of results ..........................................................................................................411

12.4 Summary of contributions ..............................................................................................414

12.5 Publications stemming from the research ........................................................................418

12.5.1 Journal Publications ..................................................................................................418

12.5.2 Conference Publications ..........................................................................................418

12.6 Limitations of this research ..............................................................................................419

12.7 Suggestions for further research ......................................................................................419

References ..................................................................................................................................420

Appendix List ...........................................................................................................................435
List of Tables

Table 3.1: Summary of the results for the literature review’s broad thematic questions ..........102
Table 3.2 Analysis of the results for the literature review’s broad thematic questions ..........105
Table 4:1: Summary of Research Design Choices .............................................................120
Table 5:1 Brain-compatible principles ..............................................................................134
Table 6:1 School participation in the SACSAA campaign and competition each year ..........164
Table 8:1 Brain-compatible principles to be applied ..........................................................185
Table 8:2 Password lessons of Do’s and Don’ts ................................................................192
Table 9:1 Number of poster entries from other schools (recommended implementation):
  Cycle 2 ..........................................................................................................................277
Table 9:2 Number of poster entries from other schools (teacher-oriented implementation):
  Cycle 1 – Cycle 2 .........................................................................................................278
Table 10:1 Number of poster entries from other schools (recommended implementation):
  Cycle 2 – Cycle 3 .........................................................................................................346
Table 11:1 Number of poster entries from other schools (recommended implementation):
  Cycle 2 – Cycle 4 .........................................................................................................388
Table 12:1 Actionable knowledge reference table ............................................................416
List of Figures

Figure 1:1 Layout of the Thesis ................................................................. 9
Figure 2.1: The relationship between information and communication security, information
security, and cybersecurity ........................................................................... 25
Figure 2:2: Levels of Culture. Adapted from Schein .................................. 30
Figure 2.3: Organisational Culture Change Process ................................. 36
Figure 4:1 The Research Onion ................................................................. 110
Figure 4:2 Case Study Process (linear but iterative) ................................. 115
Figure 4:3: Action Research Process ......................................................... 116
Figure 5:1 Hall's (1981) “circuit of television” ........................................ 151
Figure 5:2: Encoding and decoding of broadcast structures ....................... 152
Figure 6:1 Action Research Model ............................................................. 165
Figure 6:2 Action research cycles from 2011 until 2015 ............................ 168
Figure 7:1 2011 SACSAA campaign and poster competition advertisement 174
Figure 8:1 Cycle 1 action planning section outline ..................................... 183
Figure 8:2 Single topic awareness-raising posters provided as supporting material 187
Figure 8:3 Snakes and Ladders password security themed board game ........ 191
Figure 8:4 Cybersafety Pledge Form .......................................................... 194
Figure 8:5 Cybersafety 101 flyer provided as educational material ............. 195
Figure 8:6 SACSAA logo included in campaign material .......................... 199
Figure 8:7 Cyber Guardian Sid the cybersecurity and safety robot mascot .... 200
Figure 8:8 Cyber Sid Cyber Awareness Sticker .......................................... 201
Figure 8:9 Example of a poster with a fully internalised message ............... 207
Figure 8:10 Example of a poster with message “Rephrased in own terms” ...... 208
Figure 8:11 Example of a poster with a message depicted “As Given" ........... 209
Figure 8:12 Example of a poster with a message which was not internalised .... 209
Figure 8:13 Cycle 1 results and evaluation section outline ......................... 216
Figure 8:14 Percentage of School A’s competition posters per topic: Cycle 1 .......... 218
Figure 8:15 Percentage of School A’s posters relating to specific categories of device:
cycle 1 ........................................................................................................... 219
Figure 8:16 How well School A’s learners internalised the cybersecurity or cybersafety
messages: Cycle 1 .......................................................................................... 221
Figure 8:17 Percentage of School A’s posters depicting branding symbols: Cycle 1 .......... 222
Figure 8:18 Percentage of School A’s learners who answered all questions correctly........224
Figure 8:19 Percentage of Other Schools’ competition posters per topic: Cycle 1........228
Figure 8:20 Percentage of all schools’ competition posters per topic: Cycle 1........235
Figure 8:21 Percentage of all schools’ posters relating messages to specific device
categories: Cycle 1 ........................................................................................................236
Figure 8:22 How well all the schools’ learners internalised the cybersecurity or cybersafety
messages: Cycle 1 ........................................................................................................237
Figure 8:23 Percentage of all schools’ posters depicting branding symbols: Cycle 1 ..........239
Figure 9:1 Cycle 2 action planning section outline................................................................255
Figure 9:2 Additional 101 Subject-Specific Awareness-Raising Flyers ................................257
Figure 9:3 2013 SACSAA Cybersecurity calendar with past winners’ posters ..................258
Figure 9:4 Cycle 2 results and evaluation section outline .....................................................270
Figure 9:5 Percentage of School A’s competition posters per topic: Cycle 1 to Cycle 2 ....272
Figure 9:6 How well the School A’s learners internalised the cybersecurity or cybersafety
messages: Cycle 1 to Cycle 2 ..........................................................................................274
Figure 9:7 Percentage of School A’s posters depicting brand symbols: Cycle 1 to Cycle 2 ....275
Figure 9:8 Percentage of other schools’ competition posters per topic
(Recommended implementation): Cycle 2 ..........................................................................281
Figure 9:9 Percentage of other schools’ competition posters per topic
(teacher-oriented implementation): Cycle 1 – Cycle 2 .................................................283
Figure 9:10 How well other schools’ learners internalised the cybersecurity or
cybersafety messages (recommended implementation): Cycle 2 .................................285
Figure 9:11 How well the other schools’ learners internalised the cybersecurity or
cybersafety messages (teacher-oriented implementation): Cycle 1 - Cycle 2 .........286
Figure 9:12 Percentage of School B’s learners who answered each assessment's questions
correctly ...............................................................................................................................290
Figure 9:13 Percentage of School D’s learners who answered each assessment's questions
correctly ...............................................................................................................................291
Figure 9:14 Percentage of all schools’ competition posters per topic: Cycle 1 – Cycle 2 ....295
Figure 9:15 Percentage of all schools’ competition posters per topic
(Primary Schools vs High Schools) ..................................................................................296
Figure 9:16 How well all the schools’ learners internalised the cybersecurity
or cybersafety messages: Cycle 1 – Cycle 2 ....................................................................298
Figure 9:17 How well primary school and high school learners internalised the cybersecurity or cybersafety messages: Cycle 1 – Cycle 2 .......................................................... 300
Figure 9:18 Percentage of all schools’ posters depicting brand symbols: Cycle 1 – Cycle 2 ... 303
Figure 9:19 Percentage of primary schools’ vs high schools’ posters depicting brand symbols: Cycle 2 ........................................................................................................... 304
Figure 10:1 Cycle 3 action planning section outline ......................................................................................................................... 320
Figure 10:2 Past winner’s personal information security awareness poster included in current and future campaigns ................................................................. 327
Figure 10:3 Past winner’s cyber stranger danger security awareness poster included in future campaigns ........................................................................................................ 327
Figure 10:4 Redesigned and reintroduced Cyber Sid and newly introduced Cyber Sindi .......... 330
Figure 10:5 SACSAIP campaign mascot awareness badges ......................................................................................................................... 331
Figure 10:6 Cycle 3 results and evaluation section outline ......................................................................................................................... 340
Figure 10:7 Percentage of School A’s competition posters per topic: Cycle 1 – Cycle 3 .......... 342
Figure 10:8 How well School A’s learners internalised the cybersecurity or cybersafety messages: Cycle 1 – Cycle 3 .......................................................... 343
Figure 10:9 Percentage of School A’s posters depicting brand symbols: Cycle 1 – Cycle 3 .... 344
Figure 10:10 Percentage of other schools’ competition posters per topic (recommended implementation): Cycle 2 – Cycle 3......................................................... 349
Figure 10:11 How well other schools’ learners internalised the cybersecurity or cybersafety messages (recommended implementation): Cycle 3 ........................................... 351
Figure 10:12 How well the other schools’ learners internalised the cybersecurity or cybersafety messages (curriculum-oriented implementation): Cycle 3 .............. 352
Figure 10:13 Percentage of all schools’ competition posters per topic: Cycle 1 – Cycle 3 ...... 356
Figure 10:14 How well all the schools’ learners internalised the cybersecurity or cybersafety messages: Cycle 1 – Cycle 3 .......................................................... 357
Figure 10:15 Percentage of all posters depicting branding symbols: Cycle 1 – Cycle 3 ....... 357
Figure 11:1 Cycle 4 action planning section outline ......................................................................................................................... 368
Figure 11:2: Examples of classification of poster interpretation positions ................................. 378
Figure 11:3 Cycle 4 results and evaluation section outline ......................................................................................................................... 381
Figure 11:4 Percentage of School A’s competition posters per topic: Cycle 1 – Cycle 4 ........ 383
Figure 11:5 How well School A’s learners internalised the cybersecurity or cybersafety messages: Cycle 1 – Cycle 4 .......................................................... 384
Figure 11:6 Percentage of School A’s posters depicting brand symbols: Cycle 1 – Cycle 4 .... 386
Figure 11:7 Percentage of School A's posters per AAT position: Cycle 1 – Cycle 4 .................387
Figure 11:8 Percentage of other schools' competition posters per topic
(recommended implementation): Cycle 2 – Cycle 4 ........................................390
Figure 11:9 How well other schools' learners internalised the cybersecurity or cybersafety
messages (recommended implementation): Cycle 2 – Cycle 4 .............................392
Figure 11:10 Percentage of other schools' posters depicting brand symbols
(recommended implementation): Cycle 2 – Cycle 4 ........................................393
Figure 11:11 Percentage of other school's posters per AAT encoding/decoding position
(recommended implementation): Cycle 2 – Cycle 4 ........................................395
Figure 11:12 Percentage of all schools' posters per topic: Cycle 1 – Cycle 4 .......................399
Figure 11:13 Learners' internalisation of cybersecurity or cybersafety messages:
Cycle 1 – Cycle 4 .........................................................................................400
Figure 11:14 Percentage of all schools' posters depicting brand symbols: Cycle 1 – Cycle 4 ..401
Figure 11:15 Percentage of all school's posters per AAT encoding/decoding position:
Cycle 1 – Cycle 4 .........................................................................................402
1 Introduction

“Learn from yesterday, live for today, hope for tomorrow. The important thing is not to stop questioning.”

~ Albert Einstein
Chapter 1 Introduction

This chapter introduces the human factors of cybersecurity as the primary context of the study. The research problem, questions and objectives of the study are then discussed. The chapter concludes by outlining the structure of the thesis.

1.1 Background

In the current technology and information infused world, cyberspace is an integral part of everyday life. In both the personal and the professional context, cyberspace is a highly effective tool in and enabler of people’s daily digitally-transposed activities (De Lange & Von Solms, 2012; Klimburg, 2012; Siponen, 2001). Governments of several countries have recognised the many benefits that the adoption of the Internet and ICT may have for their country's welfare (Klimburg, 2012). Therefore, in many of these countries, citizens are being actively encouraged to adopt these technologies. South Africa itself has shown a rapid growth in the cyber active citizen population with the tally of active internet users (cyber citizens) growing from 2.4 million in the year 2000 to 28.5 million users in 2016 (IWS, 2017). This means that the percentage of internet penetration in South Africa has grown from 5.5% in 2000 to 52.0% in 2016 (IWS, 2017).

This rapid adoption of cyber technologies and services has had some very positive results. Examples include access to many beneficial and convenient services, utilities, and opportunities for transacting, communicating, learning, socialising, and many other activities. However, it has also had some negative and often unintended consequences. A common, problematic consequence is that citizens are becoming increasingly technology dependent while at the same time becoming increasingly vulnerable to cyber threats (Furnell, Bryant & Phippen, 2007).

Cyber users can be exposed to a wide variety of threats, including:

- technology or hardware-oriented threats, for example malware, spyware, hacking
- social or human oriented threats such as cyber harassment, cyber-bullying, cyber stalking, social engineering attacks
- content related threats, for example inappropriate, illicit, or manipulated content
- exposure to information threats such as oversharing or incautious sharing, or accidental sharing of personal, private, or otherwise valuable information.

These threats are constantly evolving and becoming ever more specialised. Even very cyber-secure and -aware users will never be completely immune to vulnerabilities created by the constant evolution of known and unknown cyber threats.
As the number of active cyberspace users increases so too does the chance of cyber threats finding a vulnerable target. It is often argued that the average cyberspace citizen is not sufficiently aware of or secured against the many cyber threats targeting them (Quigley, Burns & Stallard, 2015). In order to avoid becoming victims of cyber threats, it is imperative that these cyber citizens acquire the security and safety skills they need for safe actions in cyberspace (Deibert, 2012; Saridakis, Benson, Ezingeard & Tennakoon, 2016; Siiponen, 2001).

Cybersecurity is the protection of the interests of a person, society or nation, including their information and non-information based assets, which need protection from risks relating to their interaction with cyberspace (ISO/IEC 27032, 2012). Humans and their societies are part of the assets requiring protection. Many security specialists and national policy documents are acknowledging the need for people to be aware of, and educated about, being more cyber secure. In order to achieve this within current populations and to ensure continuity in future generations, a “self-renewing” belief that affects behaviour is needed. In an organisational context, the fostering of an information security culture addresses this need. Similarly, in a societal context, a parallel culture of cybersecurity ought to be fostered.

Education is a key contributor to the fostering of culture. Klimburg (2012, p. 133) believes that “cyber security at the national level will fail when there is an inappropriate level of cyber security awareness and education”. Security awareness’s main purpose is to influence security decisions and the adoption of secure behaviours (Bada & Sasse, 2014; Slonje, Smith & Frisén, 2013).

All cyber users who are exposed to the risks of cyberspace must be educated about cybersecurity. Cybersecurity and cybersafety awareness and educational campaigns should include all members of society and should range from primary and secondary school level to awareness campaigns aimed at adults and the elderly (Klimburg, 2012). This education is particularly important for children who interact with cyberspace from an early age (De Lange & Von Solms, 2012; Ktoridou, Eteokleous & Zahariadou, 2012; Reid & Van Niekerk, 2014; Von Solms & Von Solms, 2014).

It is likely that the children of current and future generations will interact with cyberspace in many roles and capacities throughout their lifetime. They will thus need cybersecurity knowledge and behaviours throughout their lifetimes. Cybersecurity practices should ideally be taught as an essential life skill to these children from the moment they begin interacting with cyberspace. For this reason, cybersecurity awareness campaigns and educational efforts that target children are essential. These campaigns will teach children the knowledge and skills that will form their
fundamental understanding of cybersecurity. It is extremely important that these campaigns are
designed and implemented to communicate their content in a manner that encourages the target
audience to receive and interpret the knowledge as intended by the campaigns content creators.

This study’s purpose was to contribute to the field of cybersecurity education by offering insight
into how to design and implement a cybersecurity and cybersafety campaign targeted at school
learners.

1.2 Fields of Study

The study reported on in this thesis primarily addressed issues of interest in the fields of
cybersecurity education that affect the fostering of a culture of cybersecurity.

1.3 Problem Statement

The need for a culture of information security has moved beyond its traditional organisational
boundaries (Section 1.1). Cybersecurity and its related culture are becoming a necessity for all
information and ICT users. These users include both organisations and private users.

Many countries are recognising the need for their citizens to be cyber-aware and cyber-safe. As
such, they are beginning to implement national cybersecurity campaigns and efforts (Klimburg,
2012). Existing literature recommends that these campaigns should aim to foster a national
cybersecurity culture (Klimburg, 2012).

A contributing factor to the fostering of a culture of information security is the implementation of
an information awareness, training, or education effort. In a cybersecurity campaign, an
educational endeavour is an important part of the solution. Cybersecurity at a national level would
fail without an appropriate level of cyber awareness and education (Klimburg, 2012). For these
reasons, it is important to design, implement and support a cyber-awareness and education effort
and to make it as successful as possible.

Most existing information security and cybersecurity education campaigns limit their scope.
Literature reports mainly on primary businesses, government agencies and tertiary education
institutions. These campaigns are based on culture fostering processes originally designed for
organisations. Campaigns aiming to encourage a culture of information security within an
organisation are often limited to a single context, purpose, process, and target audience. As far
as scope is concerned, many differences exist between an organisational and national societal campaign. Similarly, many differences exist in campaigns that foster a culture of information security as opposed to a culture of cybersecurity.

Information security education endeavours are afforded some guidance for their implementation by standards and guidelines such as NIST 800-12 (2004), NIST 800-16 (1998), NIST 800-50 (2003) and, for Information Technology specific audiences, the ACM/IEEE Curriculum Guidelines. In addition, various literature resources address aspects of this issue. In contrast, very little literature has addressed cybersecurity education for school learners. A comprehensive review of literature in this field is presented in Chapter 3. As far as can be determined

There is a lack of broadly recognised and detailed guidance for the design and implementation of cybersecurity awareness, training and or education campaigns in a societal context.

1.4 Thesis Statement

Efforts that aim to foster a culture of cybersecurity should be built upon well-designed and implemented cybersecurity education campaigns.

1.5 Delineation

Education is widely acknowledged as having a significant role in any culture fostering process. This research was conducted in the sphere of education in order to contribute to the fostering of a culture of cybersecurity. The particular area of interest relates to the theoretical basis and considerations required in the design, implementation, and evaluation of these campaigns.

This research examined the factors, issues and processes that should be considered when designing, implementing, and maintaining a cybersecurity awareness and educational campaign. This study recognised these issues and recommended theoretical concepts, components and strategies that could address them.

Ideally, all users in a society should be aware of their need for cybersecurity knowledge, behaviours, and solutions. However, designing and implementing an education campaign that
targets society in its entirety was beyond the scope of this study for reasons of practicality. The research focused therefore on a sub-audience within society, school learners.

As mentioned in Section 1.1, children are a particularly important part of the cybersecurity education target audience. They will be increasingly exposed to information, ICT, and an info- and cyber-centric society throughout their lifetimes. This generation of children is growing up as digital natives. Children’s lives will be enhanced by cyberspace, as they are enabled by it and make use of the opportunities and experiences it affords. However, they will also be targeted by deliberate and coincidental threats that are also enabled by cyberspace. For this reason, children will need cybersecurity and cybersafety knowledge and behaviours as life skills. These life skills should be instilled as early as possible in a child’s cyber activity and behaviour.

This research elected to target children who were attending school, since this was seen as the most practical and accessible approach to addressing a large audience of children. Initially all school children of all ages attending primary school (ages 5 to 13) or high school (ages 13 to 18) were part of the target audience. However, in Cycle 3 (2014) the research focused its efforts on primary school children as a target audience. The target audience addressed during this research is further discussed in section 6.3.2 as part of the research process. The exact target audiences who participated in the campaign each year are described in each action research cycle (section 7.3, section 8.3.1, section 9.3.1, section 10.3.1, and section 11.3.1).

1.6 Research Questions

Research aims to find “answers” to “things” in a way that is purposive and systematic (Saunders, Lewis & Thornhill, 2009). In order to find answers, however, there must be a question or many questions. These questions aid in the delineation and focus of research in order to fulfil the purpose of a study. This section introduces the questions addressed in this study. The questions were formulated after conducting the literature review presented in Chapter 2 and Chapter 3. The questions are presented here in order to maintain the expected flow of the thesis.

The primary research question was:

“**What factors should be considered when designing and implementing education campaigns that educate school learners about cybersecurity?**”
In order to answer this primary research question, the following sub-questions were asked:

<table>
<thead>
<tr>
<th>Secondary Research Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RQ1</strong></td>
</tr>
<tr>
<td><strong>RQ2</strong></td>
</tr>
<tr>
<td><strong>RQ3</strong></td>
</tr>
</tbody>
</table>

### 1.7 Research Objectives

In accordance with the research rationale, delineation and questions, the primary objective of this study was to:

**Produce actionable knowledge, which offers guidance for designing and implementing education campaigns that educate school learners about cybersecurity and cybersafety.**

In order to achieve the primary objective, the following secondary objectives were addressed:

<table>
<thead>
<tr>
<th>Secondary Research Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RO1</strong></td>
</tr>
<tr>
<td><strong>RO2</strong></td>
</tr>
<tr>
<td><strong>RO3</strong></td>
</tr>
</tbody>
</table>
1.8 Research Methodology

A detailed discussion of the methodology followed in the process of this study is provided in Chapter 4. However, for the purpose of providing context to the research questions and objectives, this section briefly introduces the main research strategy.

This study was conducted primarily using an action research strategy. Action research aims to solve current practical problems while contributing to a scientific knowledge base (Baskerville & Myers, 2004). It enables learning during the process for both the researchers and the subjects within the context of the subject’s social system (Baskerville & Myers, 2004).

As a research strategy, action research is open-ended. It does not begin with a fixed hypothesis. The research process is developmental. It involves:

- identifying a problematic/interesting issue or idea
- conceptualising a possible solution
- trying the solution
- evaluating it to see whether it aligns with the researcher’s desired result
- changing practice based on the evaluation’s results (Lewin, 1946; Saunders et al., 2009).

The process can involve multiple iterations.

Action research was judged to be suitable in addressing the research problem because of its open-ended nature and because it has been shown to be useful in research areas that relate to those addressed in this study (Baskerville & Myers, 2004). Action research has been used in organisational development and education as well as information systems research (Baskerville & Myers, 2004).

1.9 Structure of the thesis

This section is a conceptual roadmap of the thesis’s report on the research conducted in this study. Figure 1.1 provides the graphic overview of the structure and the relationships between chapters.
Chapter 1 provides a brief, high-level overview of the research problem addressed in the study. The study is introduced, delineated and briefly motivated. The chapter presents the research questions and objectives. Finally, it describes the structure of the remainder of the thesis.

![Diagram](Figure 1:1 Layout of the Thesis)

Chapter 2 to Chapter 3 form the initial literature review.
Chapter 2 delineates the study’s problem area from the broad context and general areas of interest. The chapter opens by outlining the context of the study. It then discusses the importance of information and the pervasive presence of information and communication technologies (ICT) in modern society and in our daily lives. The chapter focuses on the need to protect information, ICT infrastructure and every asset, activity, or behaviour they affect or by which they are affected. It acknowledges that for many years organisations have recognised and attempted to address the need to protect information and its infrastructures as this can affect business interests (information and ICT security).

The focus of Chapter 2 then shifts to the general area of interest in the study: the awareness of how all users, not just users in an organisational context, need to protect their information, ICT infrastructure and every asset, activity, or behaviour they affect or by which they are affected (cybersecurity). The chapter identifies children as being a particularly significant group that needs these cybersecurity skills.

Chapter 2 goes on to disambiguate the practices of information security (organisations) and cybersecurity (society). Cybersecurity extends beyond information security although it builds upon many fundamental information security concepts and processes. Addressing the human factor of cybersecurity is the study’s area of interest.

Organisations address the human factor of information security to a significant extent by fostering a culture of information security. The chapter posits that cybersecurity should learn from information security and endeavour to foster a culture of security. The process of fostering an information security culture is discussed. Details of how the process of fostering this culture may differ for cybersecurity and information security are provided.

The discussion indicates that education is a key contributor to the fostering of this culture. A lack of comprehensive guidance on how to design and implement cybersecurity campaigns is the problem area that the study was designed to address.

Determining how to design and implement a cybersecurity and cybersafety education campaign for an entire society is beyond the scope of the study. The target audience had to be more realistic. School learners were identified as societal target audience that would have a lifelong need for cybersecurity. Thus, Chapter 2 concludes by limiting the study to focus on the design and implementation of cybersecurity and cybersafety education campaigns for school learners.
Chapter 3 explores literature that contributes to a discussion of the study’s problem area. It presents a detailed review of literature providing recommendations for the design and implementation of cybersecurity and cybersafety education campaigns or reporting on existing information security or cybersecurity and cybersafety education campaigns. Lessons learned from information security education campaigns are considered. The review includes relevant information from literature on security education. The review was not limited to material applicable to school learners. The factors considered in designing and implementing a cybersecurity and cybersafety awareness, training or education campaign based on literature are the output of this chapter.

Chapter 4 describes the research process and philosophy. First, the chapter discusses the philosophical considerations of the study. Secondly, it presents the study’s choice of research paradigm and methodologies in a layered explanation approach known as the “research onion” (Saunders et al., 2009).

Following the initial literature studies, action research was conducted to investigate how various changes to the design and development of the SACSAA cybersecurity and cybersafety education campaign targeting school learners would affect learners’ existing knowledge. The thesis is structured to present separately the theoretical basis of the interventions executed in the action research process and the narrative of the action research process and its results.

Chapter 5 discusses literature on the theories underpinning the interventions executed in the action research process. These theories support Chapter 6’s actions.

Chapter 6 presents the action research process undertaken to achieve the thesis’s primary research question. Action research is a cyclical approach to research. It involves planning what to do, the intervention, and evaluating the results. The entirety of several cycles of the SACSAA cybersecurity and cybersafety campaign in the context of a longitudinal case study are presented as separate chapters for each action research cycle. Chapters 7 to Chapter 11 each present an action research cycle. Each chapter outlines an iteration of the campaign, and the changes and interventions undertaken in the action research process. The problems of each cycle are examined as well as the intervention details, the interpretation of the actions’ results and the lessons learned or confirmed within itself. Points to consider in the design and implementation of cybersecurity educational campaigns that aim to contribute to the fostering of a culture of cybersecurity amongst school learners are discussed. The lessons learned concern the actionable knowledge gained from this study that should be useful for both academic and
practitioner communities who aim to use an educational advocacy campaign to aid in the fostering of a culture of cybersecurity and cybersafety amongst school children.

Chapter 12 concludes the thesis. The chapter presents a summarised overview of the specific contributions of the research project. It links the findings and contributions to the research questions and objectives. Finally, it highlights future research opportunities.
2 Information Security and Cybersecurity

“Our technological powers increase, but the side effects and potential hazards also escalate.”

~ Alvin Toffler
This chapter presents the context of the study and the relevant background detail needed to understand it.

2.1 Introduction

Chapter 1 introduced the primary research focus for this thesis as an investigation of what factors to consider when designing and implementing education campaigns that educate school learners about cybersecurity.

A literature review is a systematic examination of relevant research conducted in a study’s field of interest. The purpose of this chapter is to present a narrative of literature that assists in establishing the context of the topic addressed by this thesis and rationalising the significance of the problem (C. Hart, 1998). The chapter is structured using inverted pyramid organisation of the literature and argument (Ferfolja & Burnett, 2009). It begins with a discussion of the context of the study from a broad perspective. Then the chapter starts to narrow in on the study’s primary focus area.

This chapter begins by discussing the broad context of the study. It outlines society’s dependence on ICT and the cyber threats that target users via its use. The need for all users to be cybersafe and cybersecure is established. Information security and cybersecurity are considered as solutions that meet the need for security. The two practices are disambiguated from a high-level view. The chapter then outlines the general procedure followed for effective solutions. The focus of the chapter then shifts to how these two types of security deal with the role of humans within their processes. It discusses societies need for a cybersecurity culture. The chapter concludes by highlighting that education is a major part of dealing with the human factor and contributing to the fostering of a culture. The chapter aims to highlight the need for an educational campaign that can help in fostering a cybersecurity culture. Finally, it scopes the practical version of a study focused on cybersecurity education campaigns targeting children (particularly school learners).

2.2 Context of the Study

Cyberspace is being adopted by humans at a rapid rate. As of March 2017, 3.7 billion people are using the Internet out of an estimated world population of 7.5 billion people (Internet World Stats, 2017). This shows a 936% growth in internet users since 2000 (Internet World Stats, 2017). Unfortunately, most people are unequipped to deal with the threats posed against them via
cyberspace. It is necessary to make users aware of these threats and to educate them about how to avoid or defend themselves against cyber threats. *Individuals may be aware of the benefits of various technologies and software packages but simultaneously unaware of the threats and security risks associated with these same technologies and packages.* To effectively reduce the risk of becoming victims of cyber threats, users need appropriate security knowledge and behaviours. Users need to adapt to avoid or secure themselves against these threats. Society at large also needs to adapt. This need for adaptation follows the pattern of adopting innovations.

Diffusion of innovation theory seeks to explain how, why, and at what rate new ideas and technologies spread through cultures and social systems (E. M. Rogers, 2003). Additionally, it explains the consequences of such diffusions. The consequences of adopting an innovation are relevant to this section’s argument. Consequences can be positive or negative. A few characteristics of a consequence are examined to determine whether it is positive or negative.

Consequences of innovation adoption are categorised based on three categories of characteristics. The first category classifies it as being desirable or undesirable (E. M. Rogers, 2003). Its categorisation relates to whether it is a functional or dysfunctional consequence. The second category classifies it as being a direct or indirect consequence (E. M. Rogers, 2003). This is based on whether it is an immediate result or a result of the immediate result. The third category classifies it as being an anticipated or unanticipated consequence. This is based on whether it is a recognised and intended consequence or not (E. M. Rogers, 2003). Consequences directly affect the society wherein the diffusion of the innovation took place.

Throughout history the adoption of various technological advances has affected society, for example, the printing press, currency, the telegraph, transistors, the electric light, the steam engine, and the car. Society adopted these innovations and adapted to accommodate them. Now these technologies and their derivatives are integral components of and contributors to the existence of modern day society. The adoption of the car is briefly discussed next.

In the case of the car, people gained a reliable means of personal travel. They could travel further with fewer inconveniences than before, and many business opportunities arose from this. Regrettably, many unanticipated and undesired consequences also occurred.

Problems that went with the adoption of the car included risks to safety, trade, and continued productivity. Examples of these problems include the following:

- Car accidents could occur if pedestrians or other cars were not considerate of one another.
• The conditions of roads affected where people were willing to travel.
• Businesses began to invest more in services that made use of the innovation rather than those that did not.
• Crimes targeting the technologies came into existence, for example, car theft, vandalism, etc.

To counter or prevent the various risks, society itself had to adapt to accommodate the technology. Adaptations have occurred through many ongoing changes in the way society perceives the technology and the way its use is managed. These changes were direct and indirect, anticipated, and unanticipated consequences of the technologies adoption.

Consequent adaptations included society taking measures such as creating road safety laws, committing to improving and keeping infrastructures that supported or developed the technologies (for example, road maintenance), the drafting of legislature to account for the crimes relating to the technology, and educating members of society about relevant operation, maintenance, and safety rules surrounding the technology. In brief, past technological innovations, such as cars, have majorly impacted society and changed it forever. The wide adoption of cyberspace is having a similarly major impact on society.

Many changes have occurred within society to accommodate the internet as well as ICT. Consequently, over the past few decades, the diffusion of cyberspace into society has occurred rapidly. The adoption of cyberspace had several anticipated and unanticipated consequences. Some of these consequences were direct, whilst others were indirect. Thus, an ongoing process of dealing with the consequences of this diffusion is occurring.

Cyberspace is an integral part of modern-day society. It is a highly effective tool and enabler of activities. Cyberspace influences or is integrated into most facets of people’s daily lives and digitally transposed activities (Klimburg, 2012; Siponen, 2001). This integration is increasingly observable yet inconspicuous.

Cyberspace is the “complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form” (ISO/IEC 27032, 2012). It has become part of the critical infrastructure that supports:
• socio-economic growth,
• the governing of nations and sub-societies,
• the conducting of business, and 
• the exercising of human rights and freedom (Klimburg, 2012).

Desirable and anticipated consequences of the integration of cyberspace into society includes:

• the enablement of businesses and governments to generate income and employment, 
• the provision of access to business and information, and 
• the enablement of e-learning and 
• facilitation of government activities (Klimburg, 2012).

The internet and ICT, which together form the backbone of cyberspace, have become indispensable. These technologies facilitate many positive aspects of modern lifestyles (Woodhouse, 2007). However, these technologies and their vast user adoption also have negative, undesired, and unexpected consequences. These same technologies and infrastructures can be used to enable, enact, or support detrimental activities, such as information exposure, crime, espionage, terrorism, and warfare (Choo, 2011; Siponen, 2002).

Many threats to users, information, and related assets now exist to exploit ICT and ICT users in one form or another. These threats include many pre-cyber threats to people, organisations, and information and that have adapted to use cyberspace as an attack platform, as well as entirely new threats that developed alongside ICT and cyberspace. Social engineering is an example of such an adapted threat, while threats such as hacking, malware, and DOS attacks are examples of new, cyber-specific threats.

Therefore, by being active in cyberspace, users are taking many conscious and unconscious risks. Users are exposing themselves and their information to many direct and indirect threats that are potentially targeting users of ICT and its associated services. Depending on the context and scope of a situation, falling victim to these threats can potentially result in negative consequences for the users as well as larger communities, such as organisations or general society.

The adoption of cyberspace, like the adoption of technologies such as the car, is causing a period during which society must adapt. Society must adjust to all consequences (desired or undesired, direct, or indirect, anticipated, or unanticipated) of the adoption. Therefore, as vehicle safety and security measures had to become part of society’s knowledge and behaviour when society
adopted vehicles, cybersafety and cybersecurity behaviours must become part of ICT use. These practices will help secure both the users and related entities’ information and other assets.

In the context of cyberspace and technology adoption, it is important to adapt to consequences that impact the security and safety of any type of asset. In relation to information and cyberspace, this is mostly dealt with through the implementation of information security and cybersecurity solutions.

Organisations have recognised the importance of securing information for several decades. Information and information technology are enablers of most processes in an organisation. Information can be considered as “the lifeblood of modern organisation and core to most business processes” (R. Von Solms & Von Solms, 2006). Information and information systems can affect a business’s competitive performance, decision-making, general work efficiency, and productivity. Losing or compromising information could lead to several negative consequences ranging from negative publicity to financial losses (Dlamini, Eloff, & Eloff, 2009). The significance of the benefits of controlling or owning information is well-acknowledged by organisations. Similarly, the significance of the disadvantages of having the information lost, compromised, or stolen is also well-acknowledged. To protect their information and related systems and processes, businesses have been implementing information security solutions. Information security is considered to be a crucial component of good corporate governance (B. Von Solms & Von Solms, 2005).

However, a limitation of this practice is that it only focuses on protecting the organisation’s (business’s) information. In brief, information security focuses on protecting all organisational information that may be used in any business activity or transaction and is considered valuable from a business perspective. However, other users beyond organisational boundaries, for example the public, also need to protect their information.

Today’s population, especially the youth, are increasingly inhabiting cyberspace. As a result, their activities, and their perceptions of cybertechnologies and their place in the world are continuously adapting. As they make use of the internet and cybertechnologies, users’ personal information is increasingly shared online by users or entities with records of users’ personal information.

Individuals within the public find that their personal information and its transactions relate to their identities, financial activities, health care, or other highly personal, private activities. By these individual users, this information is perceived as highly personal and, by extension, valuable. Personal information is shared or communicated online passively (by posting on profile pages, blogging, commenting, etc.) or interactively (via online interactions with other users in chat, email,
Exposure of personal information can be dangerous from a security and safety perspective. The detrimental effect on information may result in the “secure” information’s characteristics being compromised. This, in turn, may even lead to the individual’s personal safety being compromised, because the information that was accessed, manipulated, or stolen during the security breach may pertain directly to the user’s financial, medical, physical, or perceived safety. Accordingly, to prevent this threat to their information and any related activities, it is essential that users protect themselves and their information. This protection process must occur during both active and passive information-related activities. Thus, it is essential that individuals and/or organisations take measures to protect themselves against threats. Therefore, as these users gain access to ICT and the internet, the need to teach them to navigate cyberspace responsibly and safely becomes more urgent (Deibert, 2012). Cybersecurity and cybersafety solutions, knowledge, and behaviours are necessary for these users.

Children are subgroup of society who particularly need cybersecurity solutions and relevant knowledge and skill sets. Children are very vulnerable to cyber threats (S. Von Solms & Von Solms, 2014). Children are growing up as digital natives, surrounded by and using many digital technologies, environments, and services. However, although they are frequent users of these technologies, they are not necessarily being taught how to use them safely and securely. This is problematic, as children will continue to use ICT technologies throughout their lifetimes and will always be exposed to cyber threats. Any knowledge, skills, or resources that can help them protect themselves could be considered essential life skills for current and future children.

Typically, children look to their parents to teach them life skills. However, within our current society, many parents are ill-prepared and unaware of cyber threats, cybersecurity solutions, and cybersecurity knowledge and behaviours. Thus, although they are concerned about their children’s safety, they do not have the necessary experience, education, or expertise to teach their children to be safe and secure (De Lange & Von Solms, 2012; Lwin, Stanaland, & Miyazaki, 2008; Turow, 2001). In addition, they may be unaware of the online activities in which their children are involved (Atkinson, Furnell, & Phippen, 2009).

Children fall outside of the typical target audience for organisational information security solutions. They exist within the context of the general public or society. Therefore, a security solution that
extends beyond the context of organisations would be best suited to aid in securing them. Cybersecurity is such a practice.

This section provided an overview of the context of the study. The forthcoming sections will discuss the fields of interest in more detail. The first section will briefly outline and then differentiate the processes of information security in comparison to cybersecurity for the purposes of this study. Next, the human factor of the security processes will be discussed. The fostering of a culture as a means to address human culture will be overviewed. Finally, education will be focused on as the main area of interest for this study.

2.3 Information Security and Cybersecurity

Information and communication technologies affect the daily activities of the majority of individuals and entities within society (Klimburg, 2012, pp.2). Alongside ICT, the global internet, corporate intranets, and the World Wide Web enable a broad range of activities. The ever-expanding range of activities includes administrative tasks, research, education, public expression, art, social activity, and commerce (Crowley & Heyer, 2016). It is an enabler of many of our daily tasks. It has become an indispensable tool (Elmarie Kritzinger & Von Solms, 2010). As a result, many people, organisations, and nations have become dependent on it.

Information is “knowledge that you get about someone or something : facts or details about a subject” (Merriam Webster Dictionary, 2016). Information has been a distinguishing feature of the modern world for several decades and society is moving towards becoming increasingly information-centric (Webster, 2014). With the introduction and the rapid development of ICT, the internet, and the World Wide Web, a new “mode of information” and sharing knowledge has been enabled (Crowley & Heyer, 2016). As a result, society is moving towards becoming an information-based “e-society” (Chunying, 2010; Webster, 2014). In this e-society, the social order, economy, and critical infrastructures have become largely dependent on computer networks and information technology solutions (Jang-Jaccard & Nepal, 2014).

Furthermore, in this e-society, information permeates the personal and professional activities of users, and thus these users (members of the general public, businesses, and other facilities) all require access to information in various formats (written, printed, electronic, spoken, recorded, etc.) to conduct their various daily personal or professional transactions successfully. Accordingly, both organisational information and personal information are considered essential and important resources.
Businesses make both direct and indirect use of information in their daily transactions. It is often what information is available to the organisation that will determine whether an organisation has a competitive advantage. Accordingly, any organisational information that may be used in any business activity or transaction should be, and is, considered valuable from a business perspective. However, its value is typically of major concern only to the organisation's stakeholders and not to each employee in his/her personal capacity, as the information usually affects the business itself and not the individual employees personally.

On the other hand, individuals who make up the general public find that their personal information and its transactions relate to their identities, financial activities, health care, or other private activities. Thus, by these individual users, this information is perceived as highly personal and, by extension, valuable.

Information is an extremely valuable asset for both individuals and organisations. An asset is anything of economic or perceived value that is owned by either an individual or an organisation. Information is perceived as valuable to both organisations and individuals. Therefore, it is an asset and needs to be protected.

The protection of all assets usually involves the implementation of controls aimed at reducing risk. Assets may have vulnerabilities, which could be targeted by threats. Therefore, these vulnerabilities place the asset in question at risk. Security controls reduce risk by minimising those risks that may arise because of vulnerabilities. There may be negative consequences if an asset is compromised by a threat. An example of a possible negative consequence arising from a breach of information security would be the information either declining in value or losing the value it has for the information owner, while providing value to the source of the threat. Information can be of significant value to individuals other than its owners. The current frequency of cyber-attacks, identity thefts, and phishing attacks attest to this fact (Conklin & White, 2006).

Processes that can be used to protect information through the implementation of various controls are information security (organisations) and cybersecurity (society). This study will focus on cybersecurity. However, its understanding of how cybersecurity builds upon and extends information security is important. The remainder of this section will provide an overview of the process of information security. Then cybersecurity will be disambiguated as a separate practice.
Chapter 2 Information Security and Cybersecurity

2.3.1 Information Security

Information security is a process involving the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities (ISO/IEC 27013, 2012; Mitnick, Simon, & Wozniak, 2002). It is a type of security that is typically implemented in an organisational context (Ahlfeldt, Spagnoletti, & Sindre, 2007). For this thesis the term information security will refer to the type of information security typically practiced by businesses, whilst cybersecurity will refer to information security and related security practices practiced by users beyond organisations.

Information security involves the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording, and destruction (Allen, 2001). The overall objective of information security is the preservation of the balance between the confidentiality, integrity, and availability of information and information resources (Pfleeger, 1997). The protection of these information characteristics has become an essential tool in the maintenance of any competitive edge, cash flow, profitability, legal compliance, and commercial image to be gained or derived from the ownership of information (ISO/IEC 27013, 2012). Comprehensive information security solutions involve multifaceted physical, procedural, and logical forms of protection for the information in question.

2.3.1.1 The Process of Information Security

“Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organisational structures and software and hardware functions” (ISO/IEC 27002, 2013).

The controls are required to help avoid, counteract, or minimise the security risks endangering assets, such as informational resources. These controls may be categorised as physical, technical, or operational in nature (Van Niekerk & Von Solms, 2004b). Each of these categories will now be briefly explained.

2.3.1.1.1 Physical Controls

Physical controls comprise the first category of information security controls. Physical controls refer to those controls that provide a tangible, physical layer of protection to information and information technologies. They are the oldest form of information protection. The objectives of the control mechanisms are:
• to restrict physical access to information and information technology,
• to provide a physical barrier or protection against mechanical threats, and
• to prevent physical and financial damages or losses caused by activities such as theft, vandalism, sabotage, or accidental damage (ISO/IEC 27002, 2013).

These controls aim to fulfil their roles while maintaining information and resource availability for authorized users. Common examples of physical controls include secure facilities that are locked and require a key or access code, as well as secure cables, which safeguard equipment physically. These controls are supported by technical controls.

2.3.1.1.2 Technical Controls
The second category of security controls consists of technical controls, which are composed of technological threat countermeasures. These controls are usually software and system based. The objectives of these controls are:

• to prevent unauthorised access to information resources,
• to restrict access to resources based upon allotted privileges and access rights, and
• to prevent unauthorised changes to or the copying of information (ISO/IEC 27002, 2013).

These controls aim to fulfil their roles while maintaining information and resource availability for authorized users. A common example of a technical control is obliging users to authenticate themselves and their access privileges with unique usernames and passwords before allowing them to access a resource, such as a computer system.

Both physical and technical controls are implemented and managed via operational controls. If a human uses these controls incorrectly, their implementation can become ineffective.

2.3.1.1.3 Operational Controls
The final category of recommended controls comprises the operational controls. These controls address the role(s) of human beings in the information security process. As such, operational controls include administrative, managerial, and procedural control categories that relate to the vital role(s) human beings play in the information security process. Both physical and technical controls usually require some form of human involvement and, by extension, operational controls. The objectives of these controls are:

• to provide procedures and codes regarding expected user or personnel behaviour,
• to attempt to enforce actions that are considered appropriate uses of a particular resource on the part of users, and
• to guide users in their interactions with the physical and technical controls (ISO/IEC 27002, 2013).

These controls aim to fulfill their roles while maintaining information and resource availability for authorized users. An example of an operational control could be a policy statement requiring users to lock their office door when they exit their offices or to log out of the system when they leave their computers.

Technical controls and physical security solutions are used to guard against many types of threats. They increase security by reducing vulnerabilities in the technological and physical components of a system. However, technological, and physical solutions are not a comprehensive or infallible security solution. Several threats are not technology oriented or focused. Instead, they target a greater vulnerability – the humans in a system (Alhogail, Mirza, & Bakry, 2015; Vroom & Von Solms, 2004). This human element of security solutions needs to be addressed (Van Niekerk & Von Solms, 2010a; S. H. Von Solms, 2006).

This thesis is interested in the human factor of cybersecurity rather than information security. Therefore, before the human factor can be discussed further, cybersecurity, as it is understood for this thesis, must first be outlined. The next section will outline cybersecurity and discuss its human factor.

### 2.3.2 Cybersecurity

The concepts of information security and its relevant practices and procedures are constantly evolving to suit the fluid business environment. However, the mere implementation of information security solutions by organisations is insufficient (Siponen, 2001). The world outside of organisations has become progressively more information and information system oriented and, as a result, information security principles have become more applicable to information use in a personal context, and to systems and networks beyond businesses. At present, *all internet and ICT users* need to have at least a basic level of cybersecurity awareness and knowledge to be able to perform their daily activities securely (Chen, Medlin, & Shaw, 2008; S. H. Von Solms, 2000). This has led to the defining of another type of security, namely cybersecurity.
Traditionally, organisations have implemented some form of protection for information resources in the form of information security. However, as the boundaries of information usage moved beyond the organisational context, so did the associated risks. Information-based risks and other cyber risks are increasingly relevant to all levels of society. Security issues now require a more coordinated and focused effort from national and international society, governments, and the private sector (Dlamini et al., 2009). Consequently, based on the previously discussed definition, the need for information security has been superseded by the need for cybersecurity within this larger societal context.

Von Solms and Van Niekerk (2013) illustrate the relationship between information security, ICT security, and cybersecurity in the diagram shown in Figure 2.1. This thesis will be using the differentiation between the types of security that is depicted in Figure 2.1.

![Figure 2.1: The relationship between information and communication security, information security, and cybersecurity](image)

Thus, information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities (R. Von Solms & Van Niekerk, 2013). Comparatively, cybersecurity is the protection of cyberspace itself, including all entities that function in cyberspace and any of their assets that can be reached via cyberspace (R. Von Solms...
The boundaries of cybersecurity and the risks it protects against are greater than those of information security. In a societal context (which encompasses organisations and individuals), the risks and threats faced by users are more encompassing than those addressed by typical information security. Therefore, in a societal context, it is necessary to look beyond the organisational information security boundaries.

Sharing much of the scope of information security, cybersecurity principally involves the protection of information and ICT. However, its scope also extends much further (ISO/IEC 27032, 2012). Cybersecurity involves the preservation of the confidentiality, integrity, and availability of information in cyberspace (ISO/IEC 27032, 2012). Cyberspace is a “complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form” (ISO/IEC 27032, 2012). Therefore, in actuality, cybersecurity involves the protection of the interests of a person, society, or nation, including their information and non-information-based assets that need to be protected from risks relating to their interactions with cyberspace (R. Von Solms & Van Niekerk, 2013). As the definition of cybersecurity states, “humans and human societies have grown to become part of the assets that need to be protected” (R. Von Solms & Van Niekerk, 2013). Therefore, as with information security, humans are still considered to be both a threat and a vulnerability. However, in cybersecurity, they are also considered to be an asset that needs protection in cyberspace (ISO/IEC 27032, 2012).

2.4 The Human Factor of Cybersecurity

For “each and every company and organisation, regardless of its size, location, culture or type of business, ‘people’ are always the key factor for the success of information security management” (Eminağaoğlu, Uçar, & Eren, 2009). This will be true in cybersecurity too.

Humans have an important role in any holistic information- or cybersecurity solution and its management (Albrechtsen, 2007). People are involved in numerous ways with the design, implementation, application, and breaching of security solutions. As the human factor of the security mechanisms, these people can positively and negatively affect the effectiveness of the solutions.

Although processes and technologies can be created to be theoretically secure, how secure they truly are is dependent on the people involved in their use and implementation (Furnell & Thomson,
2009a). Furthermore, whether people use the technologies in a secure manner and follow the secure processes completely and correctly can drastically affect the extent to which these components are secure. People can consciously and unconsciously become a threat to any information security solution (Thomson, Von Solms, & Louw, 2006). As a result of this failing, many authors acknowledge that the people involved are the weakest link in information (and cyber) security (Adams & Sasse, 1999; Ashenden, 2008; Beauthement, Sasse, & Wonham, 2008; Furnell & Clarke, 2012; Furnell & Rajendran, 2012; Furnell & Thomson, 2009a; Schlienger & Teufel, 2002; Thomson et al., 2006; Van Niekerk & Von Solms, 2010b; S. H. Von Solms, 2000).

The effectiveness of a cybersecurity solution will be very dependent on users’ behaving securely and safely. However, if they do not have the underlying knowledge to inform their behaviour, secure behaviour is unlikely to occur. Users need to be aware of their own responsibilities in protecting the information, ICT, and cyberspace activities they use from external threats (Desman, 2003) to meet the requirement of behaving securely (Albrechtsen & Hovden, 2010). Therefore, two important dimensions of the human factor within cybersecurity need to be addressed, namely knowledge and behaviour.

The first dimension of the human factor that needs to be addressed is knowledge. All users need at least a basic understanding and awareness of:

- what risks they are taking in their activities
- what threats could target them
- what the potential consequences of falling victim to the threats are
- what they should do and how they should behave

The second dimension of the human factor that needs to be addressed is behaviour. Users can contribute to a security solution by securing their own behaviour and reporting society incidents that they are aware of (Albrechtsen, 2007). This is possible only if they have the necessary prerequisite knowledge. However, once users have the requisite underlying security knowledge, it does not necessarily guarantee they will display the expected security behaviours. The “human challenge” in relation to behaviour also needs to account for individuals’ unique attitudes, beliefs, and perceptions, which they bring with them to any context that requires security (Ashenden, 2008). These unique characteristics all form part of a culture.

Culture “drives most of our behaviour both inside and outside organisations” (Schein, 2009). This is true for information security culture too (Adele Da Veiga, Martins, & Eloff, 2007). Researchers
who study the human factors in information- and cybersecurity commonly acknowledge that the requisite behaviour can be attained only through the fostering of a supporting culture of information (and cyber) security (Albrechtsen & Hovden, 2010; Adele Da Veiga, 2008; Adele Da Veiga & Eloff, 2010; Furnell & Thomson, 2009a; Martins & Eloff, 2006; Schlienger & Teufel, 2003; Van Niekerk & Von Solms, 2005; R. Von Solms & Von Solms, 2004; S. H. Von Solms, 2000).

2.5 Information Security Culture to Cybersecurity Culture

Organisations often try to manage the human factor of information security by fostering an information security culture. This section presents the stance that cybersecurity should learn from information security and aim to foster a security culture. The process of fostering an information security culture (ISC) is discussed in the next section. The discussion includes an explanation of how some of the details of the process may differ when fostering a cybersecurity culture (CSC).

2.5.1 Information Security Culture

Culture is broadly considered to be the overall, taken-for-granted assumptions that a group has learnt throughout history (Schein, 2009). It emerges over time and is visible in views and actions that reflect a belief (Schlienger & Teufel, 2002). ISCs build on this premise.

Organisations have acknowledged the need for an ISC within a business context. In the past, it was found that the technical and procedural components of an information security solution were not in themselves sufficient to address the human aspects of information security (S. H. Von Solms, 2000). This led to the recommendation to embed security in the organisation through the institutionalisation of information security. Von Solms called this the Third Wave of security (S. H. Von Solms, 2000). One aspect of this institutionalization of security involved cultivating information security as a corporate culture. This includes information security standardization, international information security certification, the implementation of metrics to continuously and dynamically measure information security aspects in a company, and the cultivation of an information security culture as a corporate culture (S. H. Von Solms, 2000). These recommendations have since been and continue to be implemented, improved, and researched.

Many authors have dealt with the topic of ISC (Adele Da Veiga & Eloff, 2010; Furnell & Thomson, 2009a; Schlienger & Teufel, 2002; Van Niekerk & Von Solms, 2006; Vroom & Von Solms, 2004). Most of these authors focused on cultivating, assessing, or auditing a culture. To achieve this, the
authors had to explain what they considered to comprise an ISC. Literature shows that they commonly based their understanding and representation of an ISC on adaptations of Schein’s three-tier organisational culture model (Schlienger & Teufel, 2003).

The tiers of Schein’s organisational culture model consist of underlying assumptions, espoused values, and artifacts (Schein, 2009). However, this model deals with organisational culture in general, not ISC specifically. Schlienger and Teufel (2003) do not provide in-depth explanations of how their interpretation of the adapted model translates to the context of information security. This left much about the practice to be subjectively interpreted. Van Niekerk and Von Solms bridged this gap in knowledge by presenting a conceptual model of an ISC, which expanded on Schein’s model and focused on explaining how the culture’s underlying components and processes could influence one another (Van Niekerk & Von Solms, 2010b).

Van Niekerk and Von Solms’s definition of ISC derives from and expands Schein’s organisational culture model. Schein lists artifacts, espoused values, and knowledge as dimensions of his culture model (Schein, 2009). Van Niekerk and Von Solms expanded the ISC model by concretely integrating the requisite underlying information security knowledge as a separate component in their model (Schein, 2009). This knowledge dimension was included, as the authors theorised that, in order to foster an ISC successfully (as a subculture within an organisational culture), all business activities would need to be performed in a secure way (Van Niekerk & Von Solms, 2006). Therefore, adequate information security knowledge and skills were deemed a necessary requisite to enable an employee to perform any business activity in a secure manner (Van Niekerk & Von Solms, 2010b). Accordingly, their conceptualisation (as shown in Figure 2.1) of an ISC consists of four information security-related components, namely artifacts, espoused values, shared tacit assumptions, and knowledge (Van Niekerk & Von Solms, 2010b).

The exact contents of each of the other dimensions were altered slightly to be more context-specific to ISC. Therefore, the ISC-specific interpretation of the model dimensions now refers to the following framework components:

- **Artifacts (AF)** – Detailed procedure of the organisation’s daily tasks. This dimension includes the visible structures and processes that were deemed to be “measurable but hard to decipher” (Van Niekerk & Von Solms, 2010b). Examples of these would be the architecture and security mechanisms of the company, as well as information security policies and procedures.
Espoused Values (EV) – The guidelines for what to include in a policy and subsequent ISC to adequately address the business’s needs. These include information security strategies, goals, and philosophies. In brief, the information security-related espoused justifications and official viewpoints (Van Niekerk & Von Solms, 2010b).

Shared Tacit Assumptions (STA) – The beliefs and values of the individual and collective employees. This includes their unconscious, taken-for-granted beliefs, perceptions, thoughts, and feelings. In brief, it is the layer at which people are involved and, as such, is the ultimate source of values and action (Van Niekerk & Von Solms, 2010b).

Knowledge (KW) – The necessary and required levels of information security-specific knowledge needed to perform daily business tasks in a secure manner (Van Niekerk & Von Solms, 2010b).

Figure 2.2: Levels of Culture. Adapted from Schein (1999, p. 16) (Van Niekerk & Von Solms, 2010b).

This adaption of Schein’s organisational culture has been very suitable for ISCs because, thus far, the literature has dealt with ISCs that were cultivated, assessed, audited, and so forth in an organisational context.

However, in terms of this CSC research, the use of Schein’s model may be questioned and requires further justification. Schein’s model depends on its organisational context and an understanding of how a culture can be cultivated or measured within this insulated environment.
The previous section has shown that cybersecurity extends beyond the contextual borders of an organisation. This extension of scope will likewise affect the CSC. Therefore, one should ask whether Schein's model is acceptable for use with a CSC or whether other models, such as the one offered by Hofstede (Hofstede, Hofstede, & Minkov, 2010), would be more suitable. The next section will examine these as well as other considerations for a CSC.

2.5.2 Considerations for a Cybersecurity Culture

All the previously mentioned ISC models focused on an ISC in organisations. This research focused on a CSC to address the human factor of societal cybersecurity. Earlier sections established that a CSC will likely be similar to an ISC. However, there will be some definite differences. This section will examine some of these differences as well as considerations that have to be made. The primary issues that will be discussed relate to either the CSC’s context or its components.

2.5.2.1 Context

The first significant difference between an ISC and a CSC is the context in which the culture would be fostered. Information security cultures are cultivated and managed within insulated organisational contexts. This type of context translates to being a fairly well-controlled environment with relatively predictable user behaviour, activity, and profile sets. Comparatively, with a cybersecurity solution, the culture would be cultivated within a societal scope. Within a societal context, the environment would be less controlled, user profiles would range across many skill sets, age ranges, and other variables, and the activities being performed by the users would be less predictable than within a purpose-based organisation.

These differences would affect the ease with which a culture could be established and the degree to which the users would be willing to subscribe to the culture. It is probable that attempts to foster an ISC may experience faster and more complete success than attempts to foster a CSC in society. This is because organisations tend to have a number of cultures or behaviour sets that they seek to instil within their employees. It is possible that employee exposure to a number of such continuous culture fostering processes within a particular (arguably regulated) environment may make them more amendable to accepting other cultures in the same environment. Comparatively, a societal context is less closely regulated. For example, there are broad-based culture systems, such as national culture, religious culture, etc. There are also smaller community
cultures, which are less regulated than those within a work environment. Therefore, the users are more likely to be individualistic there than in their work environments.

Within the context of an ISC, Furnell and Thomson identified a number of factors that could be theorised as affecting the users’ (who are involved in a solution) willingness to comply with the culture (Furnell & Thomson, 2009a). These factors may also affect whether a societal user would be willing to accept a cybersecurity culture. The factors that should be considered for the CSC are:

- the roles the user must play,
- the nature of the task,
- user behaviour, and
- the psychology of the users (Furnell & Thomson, 2009a).

How the various elements of an ISC and a CSC will differ will now be briefly discussed.

The role, current task, and user behaviour that users must adopt from a security perspective while completing their tasks relate to who they are and what they are doing (Furnell & Thomson, 2009a). Within the context of an ISC, the role would relate to what the users are actually expected to do as part of their job and the security responsibilities required by the job. Within this context, the role should be easily defined, as a user will be goal/task-oriented for the organisation’s work process. Therefore, a user will be expected to consider only their role and the responsibilities for their part of the task. They would not be expected to know how to fulfil roles outside their own job description. Thus, the number of roles these users may play will be limited and they will need to adopt only the culture pertaining to these limited roles. In comparison, in a personal capacity within a societal CSC, the number of roles a user may play will be dependent on the activities they as an individual elect to complete. The user may have some fixed tasks as well as many ad hoc tasks within varying contexts. This means that users within a CSC would need to be exposed to a broad culture that shows them how to adapt their roles based on a task. This factor also relates to the general user profiles involved in the culture. Within an organisation, certain age ranges, skill sets, and suchlike are expected, and thus their roles relate to these characteristics. However, in open society the types of role characteristics are infinitely combinable.

The contextual considerations that will affect the consideration of a CSC have now been determined. The next subsection will establish how the components of the cultures will differ.
2.5.2.1 Components

As a result of the comprehensiveness of Van Niekerk and Von Solms’s definition of an ISC (Van Niekerk & Von Solms, 2010b), the focus on the conceptualisation of an ISC, and the degree of similarity (relative to the explanation) between a CSC and an ISC, this thesis will adopt their definition of an ISC to discuss the similar aspects of a societal CSC.

As discussed in the previous section, Van Niekerk and Von Solms conceptualised an ISC as having four component levels, namely:

- **Artifacts (AF)**,
- **Shared Tacit Assumptions (STA),**
- **Espoused Values (EV), and**
- **Requisite Information Security Knowledge (KW).**

In the context of a CSC, it is likely that similar abstract components would also exist. However, how they translate within real-world applications as artifacts and behaviours will differ due to the scope of the context. This section will briefly examine how these cultural components could emerge differently.

- **Artifacts (AF)**

  The first component to be considered would be the artifacts (AF). This component strongly relates to the espoused values. Considerations for this component are the following: Artifacts are observed, concrete, or tangible behaviours. In other words, artifacts are what an individual can see, hear, and feel when they observe an organisation (Furnell & Thomson, 2009b). Therefore, in an ISC, examples of these would include the physical security, the information security policies, and the procedures. In an organisational context, these artifacts are capable of being very specific in their requirements. Comparatively, the artifacts of a societal CSC would involve international and national policies, laws, and other recommended best practices. Owing to the nature of these potential artifacts, they would not be as easily established or created to be as detailed as an organisation’s artifacts. This raises the question of how to communicate the more specific recommendations to the users in society.

- **Espoused Values (EV)**

  The second component to consider would be the EV. Typically, within an ISC the EV describe the values that an organisation is said to be advocating or promoting (Furnell & Thomson,
In the context of an ISC, these EV would be issued by the board of directors or the high-level management on the business's behalf. In an organisational context, they would manifest in the business's information security policy and general vision. The approach to EV would be similar within a CSC. In terms of the overall societal scope, a similar top-down approach would be necessary. However, the degree to which the EV may be heeded would more likely be dependent on the context and the users involved than it would within an organisation. In the broader society, the espoused values would likely be issued by governmental, national, or international agencies and would then manifest as a national cybersecurity culture. This would be similar to what occurs in an ISC. However, the reason a CSC may differ from an ISC in EV is that there are a number of sub-societies within societies. In these sub-societies, there may be additional representatives (i.e. top management), who may issue other EV. These EV should or could build on the higher-level specifications but not contradict them. The EV in a CSC would be notices such as rights, laws, and national policies. Therefore, they would cover very broad areas.

- **Shared Tacit Assumptions (STA)**

The third component to be considered consists of the Shared Tacit Assumptions (STA) that are shared by a group of people. The STA encompass the underlying thoughts and values that the employees of an organisation believe to be true (Furnell & Thomson, 2009b). This level of corporate culture directly influences the behaviour of employees that can be observed at the artifact level. In terms of an ISC versus a CSC, this level will be more easily measured or perceived in an organisational context. The STA among users in a society will exist. However, because users will also belong to sub-societies, they will develop individualised instances of STA. Therefore, in a CSC these STA will be more difficult to observe. Thus, determining what STA exist will be more difficult in a CSC.

- **Knowledge (KW)**

Finally, the knowledge component will have to be considered. This relates to awareness of the requisite security knowledge needed to fulfil the users’ security roles while they are completing a task. In both an organisational and societal context, the users cannot be expected to have such default knowledge. Therefore, this component raises the question of how to provide the users with access to methods to gain this knowledge. Within an organisation, education and training is part of fostering an ISC. Education would likely also be used in fostering a CSC. However, what content should be included in the case of a CSC
must still be determined, as the number of activities a user may need to perform securely is not as predictable as it would be in an organisational context.

The literature has shown that many studies on the fostering of information security cultures have been conducted, and many frameworks or guidelines have been proposed. However, these cultures are confined to an organisation’s environment and similar-sized insulated (controlled) environments. Compared to an ISC, there are no widely accepted definitions or guidelines for what constitutes a CSC. To begin addressing this gap, this section has proposed a conceptual understanding of the probable components of and the considerations for a cybersecurity culture. Although the discussion presented here is not a definition of a CSC, it does identify the questions, components, and considerations that should be taken into account when defining a CSC. One of the major considerations for a CSC would be its lack of an insulated environment, because societal boundaries are considerably broader than the organisational boundaries of an ISC. Based on this understanding of a CSC, it should not be thought of or fostered as an abstract concept to be applied to all contexts. A CSC should be defined and fostered to suit particular contexts. The next section will address how a culture is fostered.

2.5.3 How to Foster a Culture

A need to foster a cybersecurity culture exists. However, little research about how to establish such a culture has been published. This knowledge gap needs to be addressed. Many current researchers present approaches towards the fostering of an information security culture at an organisational level. However, as far as could be determined, no current guidelines exist for the design and implementation of an educational campaign that aims to contribute to the fostering of a cybersecurity culture at a societal level.

Since information security can be seen as a subset of cybersecurity, it is reasonable to assume that some of the lessons applicable to the fostering of an information security culture would also apply to the fostering of a cybersecurity culture. However, the context of a cybersecurity culture would be more diverse than that of an information security culture. To begin to understand how these processes would differ, the cultural change process that would be used within an organisational culture fostering process (Figure 2.3) is briefly outlined. It is then considered from the perspective of a societal scope.
Schein proposed that a structured change management process is necessary to change a culture in an organisation (Schein, 2009). Figure 2.3 illustrates a culture change process that was adapted from Van Niekerk and Von Solms (2005) for the introduction of both an organisational information security sub-culture and an information security education program. The depicted process will be described briefly.
• Step 1: Top management support and commitment
In the context of an organisation, a culture change process begins with top management making a commitment to the process of fostering a “new” desired culture (Van Niekerk & Von Solms, 2005). A vision for information security is created. This initial vision can be communicated via a vision statement or an awareness campaign. Subsequently, a policy, sub-policies, and procedures complying with the vision are then drafted. The aim of such a policy is to allow management to dictate the appropriate behaviour of its employees (R. Von Solms & Von Solms, 2004). The policy will form part of the organisation’s espoused values (Van Niekerk & Von Solms, 2005).

• Step 2: Define the specific business problem
The culture change must take place in a specific context. According to Van Niekerk and Von Solms (2005), to achieve information security, the specific business problem must be defined for each specific security need. This step involves assessing the current state of culture, defining the desired culture state, measuring the gap between the states, and determining the steps needed to change from the existing state to the desired state. The measurement and definitions of these states should be done in terms of the previously discussed components of culture: espoused values, artifacts, shared tacit assumptions, and knowledge (Van Niekerk & Von Solms, 2005). The plan to move between the states will require the raising of awareness of the need for the change and the education of the users to enable change.

• Step 3: Educate the employees
As part of the plan to move from the current culture state to the desired culture state a repetitive transformative change management cycle that involves educating the employees is required. Education is often the only way to convince employees and managers of the need to do things differently (Schein, 2009). This education, which can happen in the form of awareness, training, or education programs, is vital. It focuses the users’ attention on security requirements and knowledge in order to reduce their levels of unconscious, unsecure behaviour (Furnell & Thomson, 2009a). Van Niekerk and Von Solms (2005) proposed the use of an iterative outcomes-based education program. The steps for these cycles involve the following process:
  o Define the desired outcomes.
  o Define assessment metrics for each outcome.
  o Create learning experiences that will enable learners to attain the desired outcomes.
• Expose the learners to the learning experiences (i.e. educate them).
• Provide feedback to learners based on the defined assessment metrics.
• Constantly review the learning experiences and revise them where necessary.

• Step 4: Define culture change metrics
  This involves defining what would be considered as desired behaviour, so users can be judged as successful or not. These could be based on the performance level metrics defined for the educational component (Van Niekerk & Von Solms, 2005).

• Step 5: Feedback, rewards, and punishments
  Feedback would need to be provided to the educated users and may take the form of rewards and punishments where necessary.

• Step 6: Review and refine
  Finally, the culture is reviewed and refined where necessary. This includes reviewing the “governing variables (espoused values), in order to strengthen the culture and assist with the internalisation of the new culture” (Van Niekerk & Von Solms, 2005).

This is the process used for an information security culture fostering process at an organisational level. However, a similar process is needed for fostering a cybersecurity culture. However, when the scope of the context in which the process must occur changes, exact implementation details also change drastically. Factors that would affect this process at a societal level include the following:

1. The natures of the power relationships and a security policy’s role at a national level are substantially different from those at an organisational level. An organization’s security policy is present to enable the organization to achieve its goals. Therefore, the policy can be consistent across the organization. However, in societies the policies required by different subgroups e.g. financial institutions, the government, individuals in a personal capacity etc are considerably different. Thus, authoritarian stances that could be appropriate at a policy level in an organisation might not be appropriate for or easily established as parallel legislation within a national context. It is possible to dictate the behaviour of the employees via a policy within an organisation. However, should a parallel legislation be established, this would be a less acceptable practice on a societal level (R. Von Solms & Von Solms, 2004). A cybersecurity culture and solution would need to accommodate these differences.
2. Establishing parameters for and taking measurements of the state of a national culture would be infinitely more difficult. They would also be more difficult to benchmark and assess.

3. At a societal level the target audience for awareness, training, and education activities would be much more diverse than the employees of an organisation. Education targeting an entire society would involve multiple levels of content, methods of distribution, and ethical challenges that are not as problematic in an organisational context.

4. Cybersecurity at a national level is more likely a descriptive process than a prescriptive process (users are less likely to be coerced to comply). Therefore, the usual punishment or reward aspect of the transformative change management process may be more of an abstract consequence.

Based on these and other differences, the established details of the process for fostering and managing a culture would have to be changed to fit cybersecurity’s scope and traits. However, one surety is that education will be a key contributor to the fostering of a culture. This is true in the context of information security cultures and will continue to be true in cybersecurity cultures.

Education, ranging from awareness campaigns to formal and academic education formats, is vital when addressing the current cybersecurity issues that users are facing in their daily lives (Bishop, 2000). Addressing the human factor via effective user training and awareness is consistently acknowledged as a priority by many nations’ cybersecurity plans (Department of Communication, 2011; “The UK Cyber Security Strategy,” 2011; White House, 2003). Determining how to educate society about cybersecurity is an important issue. The need for awareness, training, and education efforts regarding cybersecurity in a societal context will be the focus of this research.

Guidelines are needed to assist in addressing the needs if this audience with an effective campaign and campaign strategy. Thus, this thesis will focus on the creation, implementation, and management of societal cybersecurity campaigns, with the intent of identifying actionable knowledge which may serve as guidelines for cybersecurity and cybersafety education campaigns.

2.6 The Scope of this Research

Education is described as being a key contributor to the fostering of a culture. Providing cybersecurity education has been outlined as the study's main area of consideration. A lack of
comprehensive guidance on how to design and implement cybersecurity campaigns has been identified as the problem area the study intends to address.

The success of cybersecurity at a national level is interlinked with an appropriate level of cybersecurity awareness and education successfully reaching users. Users targeted by societal awareness and educational campaigns should include all members of society. Therefore, the target audiences of awareness campaigns should range from primary and secondary school children to adults and the elderly (Klimburg, 2012).

Determining how to design and implement a cybersecurity education campaign for an entire society is beyond the practical scope of this study. The reason for this is that a societal target audience would be very difficult to reach. Research and campaign implementation processes on such a large scale would also be very difficult for a single researcher to manage. A societal target audience consists of users with numerous different ages, skill-levels, contexts, and geographical locations. Each target group may have specific vulnerabilities and threats that target them. Campaign considerations, such as suitable content, delivery, presentation, and campaign evaluation practices, need to be considered. Therefore, the study’s scope for its practical focus has been reduced to target a specific portion of the target audience.

Section 2.2 briefly outlined that children have been identified as being a part of the societal target audience that needs to be taught cybersecure and cybersafe behaviours. They are a particularly important sub-group of the target audience because they: rapidly adopt technologies, will have a lifelong need for cybersecurity, and are particularly vulnerable to cyber threats, as they take many risks in their online activities.

Although these children are “digital natives” who are quite IT-literate, there is no guarantee that they are naturally security-aware (Furnell, 2008). Therefore, educating them about cyber threats, the risks they take, cybersafety, and cybersecurity is of paramount importance. Educating them in this regard gives children the opportunity to develop safe and responsible online behaviour when they are accessing cyberspace (De Lange & Von Solms, 2012).

The rest of this thesis, particularly the practical action research component, will focus on what factors should be considered when designing and implementing education campaigns that educate school learners about cybersecurity.

The decision was made to target children who attend schools, as implementing education campaigns at existing educational facilities will enable the cybersecurity effort to gain access to a
large number of children (learners) without having to create or manage all the implementation resources by itself.

2.7 Conclusion

This chapter presented the broader context of the research conducted within this thesis. It established the need in society for all users of information and ICT to be capable of using cyberspace in a safe and secure manner. Thus, there is a need for cybersecurity.

The chapter briefly discussed how cybersecurity, which targets society, is broader than information security, which has traditionally been implemented in organisations. Numerous details of these practices were outlined. The human factor or challenge was highlighted as being a prominent issue in both practices. The fostering of the relevant culture was discussed as an established measure for addressing the human factor. Although the exact implementation details differ, education is acknowledged as playing a vital role in fostering both information security and cybersecurity cultures. Thus, cybersecurity awareness and education campaigns were selected as the research focus for the rest of the thesis.

However, the human factor of cybersecurity is much broader than that of information security. Therefore, it was necessary to scope the study to focus on educating a sub-group of the target audience. School learners were selected as the target audience for the remainder of the research. The next section will review related works in information- and cybersecurity education.
Chapter 3 Information Security and Cybersecurity Education

“Knowledge is power. Information is liberating. Education is the premise of progress, in every society, in every family.”

~ Kofi Annan
This chapter reviews literature reporting on existing information security and cybersecurity awareness, training, and educational approaches. The aim of the chapter is to provide an overview of literature related to existing campaigns while identifying factors which contributed towards the success of awareness, training, and/or education efforts. This chapter will fulfil the first secondary research objective.

3.1 Introduction

This chapter provides an overview of existing literature, as described by (Olivier, 2009), dealing with information security and cybersecurity awareness, training and education efforts. The previous chapter, identified cybersecurity awareness, training, and education efforts as key contributors to the fostering of a cybersecurity culture amongst users. The focus of Chapter 3 is examining what factors to consider in the design, implementation and management of cybersecurity campaigns based on the recommendations and reports of other authors in the field of cybersecurity awareness, training, and education.

This chapter presents a literature review. A literature review must have a purpose. This chapter’s primary purposes are to:

- to distinguish what has been done from what needs to be done, and
- to discover important variables relevant to the topic (Hart, 1998).

In this chapter, these primary purposes met by:

- providing an overview of existing information security and cybersecurity educational efforts
- extracting lessons from the literature reports relating to theoretical and practical issues (factors) within the creation, implementation, and management of a cybersecurity educational effort.

Most existing security related research deals with information security not cybersecurity. Additionally, most of this research was conducted within an academic or organisational context and does not specifically deal with children as a target audience. However, it would be prudent for researchers of cybersecurity to take heed of lessons learned from information security because there is a large overlap between these fields. Therefore, although this research focuses
on cybersecurity, and on school learners as a target audience, due to necessity it examines material relating to information security and other users. Not all of lessons learned will be applicable to this study, however they should be considered and acknowledged.

Within the literature review there were three high-level thematic questions which were considered important whilst examining the publications. The three thematic questions were:

1. Who is the educational efforts target audience?
   This question examines who was the educational effort's target audience. The question also examines whether children were the target audience.

2. What were they educated about?
   The issue of interest is whether the awareness, training or education effort taught lessons or topics which are most relevant to information security campaigns, or cybersecurity and cybersafety campaigns.

3. How were they educated?
   The question examines what specific approaches were used to teach the learners about information security, or cybersecurity and cybersafety. This examination included considering specific underlying components, issues or processes of the educational effort highlighted in the study as being important, e.g., pedagogical design, delivery or presentation recommendation and methods, etc.

The chapter will be structured in a ‘classic’ studies organisation (Ferfolja & Burnett, 2009). Outlines of the major writings regarded as significant to thesis’s area study will be provided. The outlines will briefly summarise the focus of the study or effort, and highlight key factors of the research which relate to the literatures thematic areas of interest will be outlined. The chapter will conclude with an overview discussion of the literature recommendations made for creating, views findings regarding the issues of interest.

The next section will briefly discuss the scope of the review conducted within this chapter. Then the chapter will present the individual reviews of the included literature sources. Finally, the chapter will give a full summary and discussion of the collective reviews findings before it concludes.
3.2 Scope of Review

The objective of the literature review is to examine current cybersecurity education approaches and identify factors which contributed to their success. However, literature sources which explicitly stated they were dealing with cybersecurity were scarce. Since the terms information security and cybersecurity are often used interchangeably in literature (R. Von Solms & Van Niekerk, 2013), sources which dealt with information security education approaches were also included. The examined literature pertains to information security, or cybersecurity and cybersafety, awareness, or training, or education efforts. To be thorough, and demonstrate rigour and reliability within the research process, every effort was made to include every current source that could be deemed relevant to this review.

The report covers a broad variety of sources which were systematically selected. Sources to be examined included literature from international standards, national imperatives, curriculum guidelines and current research relevant to information security, and cybersecurity and cybersafety from a cybersecurity perspective and expert origin.

There are numerous campaigns for cybersafety issues, such as cyberbullying, in the fields of psychology. These were deemed outside the scope. This is because this review looked at the larger campaign context. However, many of these sources were consulted during the action research and are acknowledged in the action research process (Chapter 6 to Chapter 11) when appropriate. Similarly, existing works that focus on single issues such as password construction, as opposed to the context of a larger campaign, are also excluded.

The literature review begins by discussing standards. The international standards, ISO/IEC 27002 (2013) and ISO/IEC 27032 (2012), and the American information standards NIST 800-12 (2004), NIST 800-16 (1998) and NIST 800-50 (2003) are reviewed. Secondly, the review then focuses on the recommendations of prominent national imperatives. Thirdly, widely acknowledged literature relating to curriculum outlines for formal education of future IT professionals, specifically the ACM IEEE Curriculum Guidelines for Undergraduate Degrees in Information Technology, was reviewed. Finally, several peer-reviewed, academic papers are reviewed.

Included literature sources were found through an extensive search of: the contents of electronic databases, including the ACM Digital Library, EBSCOhost, Elsevier Science Direct, Emerald Library, IEEE Xplore Digital Library, and SpringerLink. Particular attention was paid to the proceedings of IFIP Working Group 11.8 and 11.12 conferences when available, as the author
consider this research to be of particular relevance to the research area. In some cases, where papers from these conferences were published in journals, the journal publication was selected for review.

The review's results are relevant and current as sources published before 2000 are excluded from the review. The report includes literature published until December 2015. The last complete and fully analysed campaign cycle was conducted in 2015.

3.3 Comprehensive Review of existing information security and cybersecurity educational literature

The literature review section will begin with an examination of the factors identified and recommendations made by the various international and national standards for information security and cybersecurity awareness, training, and education (Section 3.3.1). This will be followed by a brief overview of the education-related factors and recommendations of prominent national imperatives (Section 3.3.2). A brief overview of the ACM IEEE Curriculum’s recommendations and factors will then be presented (Section 3.3.3). The fourth component of the section will review current research (Section 3.3.4). Finally, the section will conclude with the summary and discussion of the content analysis’s findings for factors and recommendations which should be considered or contribute to a successful cybersecurity awareness, training and/or education campaign (Section 3.3.5).

3.3.1 Standards

This section will discuss international standards ISO/IEC 27002 and ISO/IEC 27032. Then it will discuss relevant American national standards from the National Institute of Standards and Technology (NIST) series, NIST 800-12, NIST800-16, and NIST800-50.

3.3.1.1 ISO/IEC 27002

There are numerous standards relating to information security in general, the most prominent being the international standard ISO/IEC 27002 which was prepared by the Joint Technical Committee ISO/IEC JTC 1, Information Technology, Subcommittee SC 27, IT Security techniques (ISO/IEC 27002, 2013). The purpose of this standard is to provide a code of practice for
information security management and, as such, the standard provides guidelines and control recommendations for the implementation and management of an information security solution.

ISO/IEC27002 states that “information security is important to both public and private sector businesses, and to protect critical infrastructures” (ISO/IEC 27002, 2013). As part of its recommendations for the management of human resources during their term of employment, the standard suggests that the all employees and, where relevant, contractors and third party users receive appropriate information security awareness training and education (ISO/IEC 27002, 2013 p.26).

The purpose of the training would be to increase and enhance the cybersecurity awareness of the parties involved (learners). Accordingly, the objective of the training would be to provide the learners with the knowledge and skills required to “recognize information security problems and incidents, and respond according to the needs of their work role” (ISO/IEC 27002, 2013). This, in turn, leads on to the question of what this training should cover and how this training should be delivered and presented.

The standard states that the “selection of security controls is dependent upon organisational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organisation” (ISO/IEC 27002, 2013), while the implementation guidance provided by the ISO/IEC27002 standard recommends the creation of “a formal induction process designed to introduce the organisation’s security policies and expectations” (ISO/IEC 27002, 2013).

In order to address the question of what should be taught, the standard recommends that the course include material pertaining to the chosen security requirements, legal responsibilities and business controls of the organisation concerned, the correct use of information processing, the use of software packages and information on the disciplinary process. Thus, the standard has provided partial guidelines for the selection of the content of an awareness training programme. However, the guidelines are considered to be partial only because the standard does not indicate the specific controls which should be included nor has it emphasised education efforts targeting specific groups of users, with these issues being left to the discretion of the course creator.

In addition, the standard makes no reference at all to how to deliver and present the content. Beyond recommending that an ongoing formal education process be put in place the standard does not provide any specific details on the implementation of an awareness training course nor any guidelines on the design, development, delivery, or presentation of such a course. Thus, even
though ISO27002 may inspire and, in fact, lead to the initiation of a cybersecurity education programme, it may not be used to guide the design and implementation of the course. Accordingly, in order to attempt to address this issue it was necessary to search other standards for recommendations on the delivery and presentation of information security education material.

3.3.1.2 ISO/IEC 27032

International standard ISO/IEC 27032, is titled “Information technology — Security techniques — Guidelines for cybersecurity”. It was prepared by the Joint Technical Committee ISO/IEC JTC 1, Information Technology, Subcommittee SC 27, IT Security techniques. The purpose of ISO/IEC 27032 is “to address Cyberspace security or Cybersecurity issues which concentrate on bridging the gaps between the different security domains in the Cyberspace. In particular the International Standard provides technical guidance for addressing common Cybersecurity risks” (ISO/IEC 27032, 2012).

Overall this standard presents a general description of what cybersecurity entails. However, it is limited in detail. The standards describe controls within the solution at a high level. This International Standard recognises but does not address: Cybersafety, Cybercrime, CIIP, Internet safety, and Internet related crime. “The guidance in this International Standard is limited to the realization of the Cyberspace on the Internet, including the endpoints” (ISO/IEC 27032, 2012).

Like ISO/IEC 27002 this standard prescribes awareness and training aid stakeholders to “develop the required skills and expertise to respond effectively and efficiently when they encounter specific risk involved, or received information requiring their actions to mitigate or improve a given situation”. To achieve these objectives regular briefings, focused training sessions and regular scenario simulations. No detailed guidance is provided for what to include, how to present of how to deliver this awareness or training activities.

There are no other international standards relevant to information security or cybersecurity education although there are a few relevant national standards. The most applicable of these national standards is the National Institute of Standards and Technology (NIST) series from the United States of America.

The NIST, as part of its mission, develops standard reference materials. These standard reference materials are used as artefacts by members of industry, academia, and government as well as other users. The researcher deemed three of these NIST standards to be relevant to information security awareness, training, and education, namely, NIST 800-12, NIST800-16, and
NIST800-50. Some of their recommendations could be applicable to cybersecurity and cybersafety awareness, training, and education. These standards will be addressed briefly in this section.

### 3.3.1.3 NIST800-12

NIST800-12 is the first relevant standard which was published by the American National Institute of Standards and Technology. The standard provides an introduction to computer security and, as such, is "An Introduction to Computer Security: The NIST Handbook". “The handbook was written primarily for those who have computer security responsibilities and need assistance understanding basic concepts and techniques" (NIST 800-12, 2004, p. 3). Accordingly, the standard provides explanations and guidelines to help individuals “understand their computer security needs and develop a sound approach to the selection of appropriate security controls” (NIST 800-12, 2004, p. 3). The prioritisation and implementation of information security controls and techniques are dependent on the context in which they are being implemented. This context may include a private or professional sector user as its managing party (NIST 800-12, 2004, p. 3). Thus, although the original target audience of the standard was the federal government, the target audience of the standard may be said to include anybody in any sector who is implementing or managing an information security solution and its related controls and components (NIST 800-12, 2004, p. 3).

Chapter thirteen, “Awareness, Training, and Education”, spanning pages 143 to 152, is the chapter in the handbook which is most relevant to information security education. The recommendations and guidelines suggested in this chapter will be discussed later in this section.

### 3.3.1.4 NIST800-16

NIST800-16 was the second standard that may be considered relevant to information security awareness, training, and education approaches. This standard presents a training model which is designed specifically for information security training. The model is entitled “Information Technology Security Training Requirements: A Role- and Performance-Based Model”. When combined with the related NIST800-50 document NIST800-16 may be regarded as the document which is most exclusively focused on information security education requirements. NIST800-16 itself issues guidelines for federal computer security training and presents a new conceptual framework for providing IT security training (NIST 800-16, 1998, p. 4). The model is role-based.
and, therefore, it describes the IT security education which is required by an individual as that individual assumes different roles and related responsibilities within an organisation. The model and its implications for information security awareness, training and education efforts will be addressed later in this section.

### 3.3.1.5 NIST800-50

NIST800-50 – “Building an Information Technology Security Awareness and Training Program” – is complementary to the abovementioned NIST800-16. The purpose of NIST800-50 is to provide “guidelines for building and maintaining a comprehensive awareness and training program, as part of an organisation’s IT security program” (NIST 800-50, 2003, p. 1). Thus, guidelines are provided for the design, development, implementation and post-implementation evaluation of an awareness and training programme. As such, the document describes how to select content, find resources, implement the actual material, evaluate the programme’s effectiveness and then update and improve the programme (NIST 800-50, 2003, p. 1). For the purposes of this dissertation, NIST800-50 is the most relevant standard for addressing the creation of a cybersecurity education approach.

### 3.3.1.6 Discussion of NIST Standard Recommendations for Information Security Awareness, Training, and Education Approaches

The NIST standards recognise that people constitute one of the weakest links in both information systems and related security systems. In order to address this issue and to improve the implementation of a security solution, the NIST standards recommend that all users with access to information and related programs or technologies undergo information and information system security awareness, training, and education.

The purpose of computer security awareness, training and education is to make users aware of the necessity of protecting system resources and of developing their skills and knowledge to enable them to act in a secure manner and to provide them with the requisite knowledge of how to design, implement and operate a security programme (NIST 800-12, 2004, p. 145). In brief, computer security awareness, training and education assist in encouraging users to change their behaviour and to carry out all information and communication technology activities in a secure manner.
Collectively, the NIST standards recognise information security learning as an education continuum. This continuum consists of three planes, namely, awareness, training, and education. In a learning context the continuum context starts with awareness, builds to training and evolves into education (NIST 800-16, 1998, p. 14). The model is role-based. This, in turn, means that the model defines the IT security learning required as a person assumes different roles within an organisation and different responsibilities in relation to IT systems (NIST 800-16, 1998, p. 14). This learning continuum has been widely accepted, with several academic publications having been based on or reviewed against its definition explanations.

Each plane of the continuum will now be briefly discussed. The topics of interest within each plane will include whom to educate, what content should be included within this plane’s programmes and how this material should be delivered and presented.

1. Awareness

Awareness programmes comprise the first plane of the continuum. The purpose of these awareness programmes is to capture the attention of the target audience and to ensure that the members of this audience are aware of security issues. In other words, the aim of these programmes is to stimulate and motivate users to realise the importance of security and also to make them aware of possible adverse effects on information and infrastructure should security fail (NIST 800-12, 2004, p. 146). These programmes also seek to remind them of the procedure or actions they should execute.

As regards their content, delivery and presentation, awareness programmes may take on different forms, depending on the target audience (NIST 800-12, 2004, p. 146), with the security needs, skills and roles of the target audiences determining what is appropriate for each particular programme.

“A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign” (NIST 800-50, 2003, p. 24). Typically, the content which is included in an awareness programme provides information designed to assist users in their recognising of security threats and the appropriate countermeasures. In addition, the content is also used to remind users of basic security procedures (NIST 800-16, 1998, p. 14). In short, the content of an awareness programme deals with providing answers to the major information system questions beginning with the word “What …?” for example, “What threats exist?” “What can the user do to prevent these threats from compromising the system?” and suchlike.
Awareness programmes rely on reaching broad audiences with their attractive packaging techniques (NIST 800-50, 2003, p. 9). Techniques for the delivery of the awareness programme’s content include several teaching techniques, including video tapes, newsletters, posters, bulletin boards, flyers, demonstrations, briefings, short reminder notices at log on, talks and lectures (NIST 800-12, 2004, p. 147). The effective security awareness programme will creatively use many of the awareness techniques interchangeably (NIST 800-12, 2004, p. 148). This is to prevent audiences from becoming bored or losing interest in one approach and to maintain their interest in and focus on the issues being addressed.

Apart from suggesting delivery mediums, no presentation guidelines are provided for the awareness material.

2. Training

Training programmes comprise the second plane of the learning continuum and they build upon the information provided in the awareness programmes. The purpose of training is to provide users with the required knowledge and skills that will enable them to perform their various information activities in a more secure way (NIST 800-12, 2004, p. 148). As such, training programmes focus on teaching users what actions they should perform and how they should perform these actions. They also emphasize what actions users should not perform.

As a plane on the continuum, awareness was often adapted to suit the audience in question. However, the audience in this case was a broad audience. Training, by comparison, is the most effective when it targets a specific audience (NIST 800-12, 2004 , p. 148). The knowledge and skills taught through training may vary in difficulty, while the knowledge and skills range taught can relate to any content from basic security practices to more advanced or specialised skills (NIST 800-12, 2004 , p. 148). However, it is essential that the content taught during training be applicable to and useful in addressing security issues that directly affect the users and their own roles and responsibilities (NIST 800-16, 1998, p. 14).

The techniques recommended for the presentation of training material include various types of topic-specific training courses. These courses or course modules may be either computer- or lecture-based or a combination of the two (NIST 800-12, 2004, p. 149). Hands-on activities or exercises and case studies were also recommended as delivery techniques.
However, once again the exact presentation of details and guidelines in respect of the material were not provided. Nevertheless, it was clear that hands-on activities and case studies would require interactive presentation and delivery.

3. Education

Security education refers to an advanced form of information security training with the objective of proving an in-depth understanding of all the previously learnt concepts and skills (NIST 800-12, 2004, p. 149). “The “Education” level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles” (NIST 800-16, 1998, 16). This explains “why” information security is necessary.

Thus, the education plane of the learning continuum targets security professionals and those individuals whose jobs require expertise in security (NIST 800-12, 2004, p. 149).

Security education is typically “obtained through college or graduate classes or through specialized training programs” (NIST 800-12, 2004, 149). It’s typical delivery and presentation methods include theoretical instruction methods such as discussion seminars and background reading (NIST 800-12, 2004, p. 147).

It is possible to make several observations based on the examination of the full learning continuum. These observations include who should be educated, what they should be educated about and how the material may be delivered and presented.

The NIST model is role-based and, thus, the target audience in respect of each plane of the continuum differed. The individuals in need of the particular type of learning offered by each plane were characterised by a specific state of awareness, priorities, and roles. In terms of the initial plane which provided awareness programmes, all the employees (users) required exposure to the material (NIST 800-16, 1998, p. 14), while progress through to the training plane led to those individuals who play a role in the information security solution requiring training only. Finally, education targets current and future IT professionals.

As regards each plane of information security learning, it is clear that the target audience has an impact on the design and implementation of the course, with each plane tending to cater for the preferences of specific types of target audience. Thus, the content chosen for inclusion in the programme is dependent on the plane of the continuum and on the requirements and learning
preferences of the target audience. In addition, the objective of the programme also affects the content choice.

NIST800-16 provides a framework that consists of a “training matrix” that could be used to determine the specific training needs of individuals. This framework can be used to select what is relevant to each individual from the general curriculum provided by NIST80-16. The needs of the users are determined based on their organisational roles, the level of training they require (beginner, intermediate or advanced) and the relevant training areas, which may vary depending on the information security policy and supporting procedures of the organisation in question. For example, if the audience changed, the type of learning needed, and which was provided also changed. In addition, the content became more comprehensive and detailed as the continuum progressed.

The target audience may also affect the delivery and presentation methods of the programmes, no matter the learning plane. Individuals learn differently. “The learning approach most effective for a particular individual is a function of their preferred learning style, education, and prior experience” (NIST 800-16, 1998, p. 16). Accordingly, the NIST standards recommend taking into consideration the learning style preferences of the learners when selecting delivery and presentation techniques for course material. However, beyond this recommendation, the standards provide very few guidelines for the selection and implementation of the delivery and presentation methods of any programme. Nevertheless, the standards did provide a few examples for each plane of the continuum.

Ultimately the NIST standards provide information about the generalities of whom to educate, what to educate them about and how to deliver this education. However, the recommendations are mostly high-level conceptual suggestions and examples and no detailed implementation details are provided for the exact implementation (delivery and presentation) of an information security learning programme. Therefore, in conclusion, the NIST standards address whom to educate and what to educate them about in a fairly broad context. However, the standards do not address how to present the courses and the course material in any detail. Thus, in order to cater for this aspect of course design other sources are needed.

3.3.2 National Imperatives

Currently several countries acknowledge the need for national cybersecurity solutions. Several countries have a National Cybersecurity Imperative and/or Strategy. Cybersecurity education is
recommended as a component of most of these imperatives, although the recommendation varies in its level of detail. A review of every national cybersecurity related imperative which recommends education is beyond the scope of research. This section will thus only briefly examine a few well-known national imperatives (United Kingdom, United States of America).

1. The UK Cyber Security Strategy

This document contains the UK government’s statement of intent to implement a countrywide cybersecurity effort. However, as an initial statement, the document presents high-level plans for the implementation of the various effort components only. Accordingly, the document identifies who will be educated as a target audience but provides very little detail about exactly what content the educational component will include and how this content will be delivered and presented.

The UK security effort identifies the target audience as everyone involved in the economy of the country. This includes large organisations, smaller organisations, businesses in the private sector and individuals who are concerned about their own personal security as regards crime, fraud and identity (The UK Cyber Security Strategy, 2011, p. 5).

However, educational content requirements are not identified or discussed in any great detail and the only guideline for the content selection provided by the document is its statement that it is essential that individuals, as well as business and government employees, all know how to protect themselves from online threats and crime. Accordingly, as a minimum requirement, it is recommended that all individuals involved in security solutions know how to implement basic protection measures against online threats. In other words, the content must be presented in an accurate way and it must be abreast of current information on the online threats that individuals may face, as well as the techniques and practices they may employ to guard against these threats. (The UK Cyber Security Strategy, 2011, p. 22)

The delivery and presentation of the educational material is not addressed although an existing online education effort is cited as an example. One of the existing campaigns is known as “Get Safe Online”. This campaign is aimed at both the general public and at small businesses in an effort to raise awareness of online security (The UK Cyber Security Strategy, 2011, p. 31). In addition, plans for the creation of cyber incident exercises are also underway (The UK Cyber Security Strategy, 2011, p. 41).
2. The National Strategy to Secure Cyberspace (USA)

As mentioned in chapter 2 the purpose of the US national strategy for cybersecurity is to “engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact” (White House, 2003, p. vii). Thus, it is a document issued by the White House stating the government’s intent to encourage and implement a nation-wide cybersecurity effort (White House, 2003, p. vii).

A few of the objectives included within Priority III of the National Strategy include the promotion of a comprehensive national awareness of cybersecurity and the fostering of adequate training and education programmes designed to meet support the nation’s cybersecurity needs (White House, 2003, p. 37). The document states that the Department of Home Security, in coordination with other agencies and private organisations, “would work to educate the general public of home users, students, children, and small businesses on basic cyberspace safety and security issues” (White House, 2003, p. 39).

The target audience of this effort is the entire nation, including the federal government, state and local governments, the private sector, and the American people at large. The individuals include computer users, systems administrators, technology developers, procurement officials, auditors, chief information officers (CIOs), chief executive officers and corporate boards, all of whom must be educated.

The document provides guidance about the content to be included in awareness, training, and education efforts. However, the examples it provides do not constitute a comprehensive curriculum, nor are they comprehensive guidelines for the selection of content and controls designed in order to educate the various facets of the target audience.

In addition, the document does not address the delivery or presentation of any of the proposed awareness, training, or education programmes.

To summarise, both of the national cybersecurity efforts aim at educating all their citizens. Both statements provide examples of possible education content, although neither statement of intent addresses the details of the selection of course content or the delivery and presentation of course material. Thus, in order to guide these aspects of cybersecurity education it may be necessary to consult guidelines regarding the drawing up of information security education courses.
3.3.3 Curriculum Guidelines

Information security is taught as a subject in many formal educational programmes and institutions. In addition, it is possible to integrate its concepts into other curricula and this has, indeed, been done. Most of the formal educational institutions have devised internal curriculum guidelines for their own subjects. However, as far as may be determined, one internationally accepted guideline only currently exists for information security programs, namely, “Curriculum Guidelines for Undergraduate Degree Programs in Information Technology” and presented by the Association for Computing Machinery (ACM) IEEE Computer Society.

The ACM/IEEE Curriculum Guidelines provide a model accompanied by explanatory guidelines and principles for the creation of a four-year undergraduate degree programme in Information Technology (Lunt et al., 2008). Thus, it comprises a formal education approach, targeting a specific subset of learners, that is, university students who are formally studying computer subjects (future professionals). However, as such the specifics of these guidelines were not considered to be applicable to the wider, societal end-user based target audience of this study. Nor is it considered applicable to the education of school learners.

3.3.4 Related Research

This section will examine the academic papers that were selected in accordance with the constraints provided in the scope of the content analysis. The papers, which are reviewed and analysed in this section, are the papers which were deemed most relevant to this research.

Albrechtsen (2007) examines how organisational users perceive of their experience of information security practices and their own work-related security role within an information security solution at their workplace. The study begins by recognising that users can contribute to organisational information security through securing their own behaviours and reporting security incidents. Subsequently the aim of the paper was to measure existing user’s perceptions of their security activities. According to the authors a user’s view on information security is shaped by several interlocking organisational, technological, and individual factors. The presented research explains users’ experiences of information security by organisational factors. The users’ roles in an information security solution is discussed. Users are identified as being an important part of a solution while also being a weakness of such a solution. It is stated that important part of information security management is to deal with the human component of these solutions. It is
necessary for management to understand the users function within their work context. It is also necessary for management to determine what actions can be used to successfully influence users' behaviour and awareness. The authors note that cultural aspects of security solutions have become a focus for companies to try address human-based security issues. This has led to an increased trend of information security awareness campaigns being implemented within organisations is cited as being part of culture fostering activities. The paper then presents a practical study to measure user perceptions was then presented. The study was conducted in two organisations where information security is essential for business. A Norwegian bank and a Norwegian IT company were the context of the study. Interviews were conducted with the organisation’s administrative employees and then qualitatively analysed. Both companies had information security guidelines available for employees. The IT company had recently conducted a mass-media awareness campaign. This and previous iterations of awareness campaigns include posters, pamphlets, gifts i.e. chocolate with security messages attached. The users involved in the study did not have management positions and were selected for having low information security awareness and little information systems knowledge. It dealt with the users understanding of the organisational issues in relation to their own individual information security behaviour. The results were not generalised, and are interpretations of the actual user’s responses. The results showed that the users claimed to be aware of and motivated in their role in a security solution is important. However, their practical security knowledge and behaviours do not reflect this. Secondly, the users prioritised functionality over information security in their work activities, particularly when workloads are high. Limited time was considered a stressor on any activities where additional security behaviours, efficiency and acceptable risk was thus prioritised over ideal security. Thirdly users were not knowledgeable about the content of their companies documented guidelines for expected behaviour despite having access to documentation and an awareness campaign. Fourthly, the general awareness and attitude campaigns which the users had been exposed to were not perceived by the majority of the users as memorable or to have had an effect on their behaviour. Finally, it was concluded that the authors and users perceived a user-involving approach as the most effective tool for influencing individual security awareness and behaviour. No evidence of a particular theoretical basis for the analysis of the data was given. No evidence of a multidisciplinary approach was described within the research or campaign.

Albrechtsen and Hovden (2009) examine the “digital divide” which exists between information security manager’s and user’s views, experiences, and interpretations of information security practices. This digital divide is a result of “of differences in self-efficacy, individual skills and perceptions, cultural aspects, and interpersonal relationships, all of which contribute to a gap in
the use of information systems”. Practically the “digital divide” refers to the differences in the information security managers and users: approaches, experiences, understandings, and priorities. The divide can be examined from multiple perspectives e.g. social, psychological, etc. From a socio-technical perspective a digital divide within information security within organisations is a product of the differences in information security skills and knowledge, perceptions of information security, social norms, and interpersonal relationships between the many users and the management levels within the organisation.” All of these factors lead to differences in information security performance amongst individuals. The study explores various aspects of the roles of managers and users and explores the similarities and differences between their views and experience of information security practices in their organisations. The studies focus was on issues categorised as being non-technical, and relating more to the human aspects (user) of security. The participants were from the following types of organisations: a Norwegian bank, a Norwegian IT-company, a Norwegian public agency, and several Norwegian business organisations. The paper presents findings from studies conducted using interview studies and surveys of information security managers and users. The participants were selected due to their roles in the administrative information security systems. The viewpoints considered were the following: the role of information security managers, the role of users, administrative security measures, and finally threats and vulnerabilities. The study found that all of the businesses adopted technical solutions. Comparatively, only one agency actively involved their users in the process. Technical solutions were perceived to be more reliable. The study found that managers tended to consider the users as a threat to the solutions, whilst the users considered themselves a resource. Managers believe that few users read and adopted their organisations information security solution documents in order to become aware gain knowledge, and change their behaviour. Users stated that they were frequently aware of necessary information security requirements in their activities, however the users tended to prioritise trade off information security against efficiency and functionality. The efficiency and functionality is frequently prioritised. Managers had also noted this trend. Awareness and education efforts in various formats, which targeted the users, were implemented to different degrees at the involved agencies. However, these efforts were found to mostly ignored or unsubscribed to by the user is due to a lack of motivation and/or mindfulness of their own need for information security knowledge and awareness. All of the involved organisations had made use documentation, and simple awareness messages and campaigns to share information security messages and information with the users. All of the involved agencies had made use of awareness campaigns in the form of formal documentation (policies, guidelines etc.) and electronic messages on various platforms
(screensavers, security messages etc.). Approximately half of the agencies provide further in-depth educational efforts such as information material (newsletters, posters, leaflets, objects, etc.), gatherings (plenary sessions, information meetings, etc.) and education and competitions (interactive training and/or competitions etc.). Few or the companies made use of informal personal presence measures. Both groups, the users, and managers, had low confidence on the impact of documentation and formal one-way information measures taken to affect user awareness and behaviour. Both groups felt that measures which enables a participative approach has a higher probability of succeeding in the modification of the user’s awareness and behaviour. In summary, the differences in the users and manager’s viewpoints showed that managers showed a tendency have information security beaver expectations which could to realistically align with the users work activities. Also, while the users trusted the managers and technical solutions to secure them, the managers do not trust the users. This had led to poor communication and a lack of co-operation. Both the managers and the users concluded that a solution which involved increased interaction and dialogue between the two groups would reduce the digital divide and result in the resultant information security measures being more effective. This source provides some guidance for the delivery and presentation of awareness and education efforts by describing the educational resources used in their organisation education efforts.

Albrechtsen and Hovden (2010) examined what effect an information security training programme, which actively involved the target audience (users), had on the user’s information security awareness and behaviour. The authors believe that within the organisation there needs to be shared understanding and insight into information security structures and procedures in order to facilitate coordinated information security interaction in an organisation. Therefore, simply educated the individuals is not sufficient, and further action to allow employees to gain a shared understanding of the inter-connect aspects of information security solutions affecting them is required. An argument is made that an effort which incorporates local knowledge, involves the employees, and facilitates the sharing of thoughts and experiences may facilitate such a shared understanding, and a more unified organisational information security approach and outlook. This method is argued to be necessary and efficient for attaining organisational change. The authors conducted an intervention study within the Norwegian public administration agency, the Brønnøysund Register Centre. This study was designed to follow an experimental procedure. A control group of employees was expose to standard information security practices and awareness training, and a second group was exposed to a new awareness approach which emphasized the importance of employee participation, plenary reflections, and group for improving shared understanding of and co-operation within information security procedures etc. The intervention
group involved small 2-hour workshops each involving approximately 15 people. The workshops required users to discuss information security issues, scenarios, and scenarios amongst themselves, which created the possibility for each participant to reflect over their working situation and information security on their own terms. It also allowed them listen to colleagues’ and security officers’ knowledge in plenary reflections. The expected outcome of this approach was changes of both awareness and behaviour. The study found that the intervention’s approach with active user participation and group-oriented execution, was powerful enough to significantly change a broad range of awareness and behaviour indicators. Indicators included the users’ perception of information security related responsibility, motivation, prioritization, reporting and perceived skills and knowledge. The change of awareness was described as improved attitudes toward and knowledge of information security after the intervention, while behavioural changes were related to perceived changes of behaviour among employees. The changes had been measured as being stable for at least half a year at the time of the publication write-up. The authors identified employee participation, collective dialogue and reflections in a universally comprehensible language register based on the employees’ own terms, laid-back expert facilitators, mutual trust in small-sized groups, and sharing of locally-based tacit knowledge as key principles which led to the interventions success. Although it is not explicitly stated this effort aimed to foster an organisational information security culture. Based on the results of the study an initial culture may have begun to form.

Alnatheer and Nelson (2009) aimed to identify the conditions (issues and factors) required for creating an information security culture in Saudi Arabian organisations. The paper begins by providing an overview of information security and information security management. The authors state that information security cultures and practices have been recognised as being important by many countries e.g. USA, the UK and China. It is stated that previously conducted research and major international standards have been written from the perspective of technologically developed countries. The authors consider how the guidance given by these publications takes into consideration the effect different environments (e.g. cultural difference) can have on information security management concepts and practices. The paper then focuses on Information security in the context of Saudi Arabia. It examines information security management practices and the need for related research from the perspective of Saudi Arabian organisations and academic/private researchers. Saudi Arabia’s “National Communications and IT Plan” is briefly discussed, its aim is to guide the country into becoming an information society and digital economy. As part of this goal, the need to foster a national information security culture is identified as a focus of the research. The authors found several issues and factors that can influence the
cultivation of an information security culture. These issues and factors were identified from a Saudi Arabian perspective. They categorised as relating to the following themes: corporate citizenship, legal regulatory environment. Corporate governance or cultural factors. The corporate citizenship theme recognised the importance of raising all, IT-using, employee’s awareness of security issues is a key issue in culture formation, and can be addressed through the provision information security awareness and training programs. The authors noted that this type of corporate citizenship (awareness and training) needed to be addressed at individual, organisational and national levels. The cultural factor theme dealt with how national and organisational culture can affect the adoption of Information security culture. The authors present a conceptual framework takes into consideration how to use all of the identified factors to aid in the fostering of an information security in a Saudi Arabian environment. The authors aim to validate the framework future work. This literary source was particular supportive of considering the environment, context and other cultures which may affect the security solution, and by extension it is education programs. This paper provides guidance by recommending addressing multiple contexts, perspectives and having it influence content.

Atkinson, Furnell, and Phippen (2009) examined the need for e-safety awareness amongst the youth. The need to increase their awareness was attributed to the degree to which the youth are increasingly exposed to cyberspace and cyber activities, and the accompanying risks. The paper begins by delineating the various threats faced, and risks taken, by users when they use various technologies and then contrasted this against the degree of relative naivety users have about the dangers they face while online. The paper then explains that the typical role-models in society from whom the youth would typically learn secure behaviours etc., are not suitably equipped with their own knowledge in this area. The paper then discusses how technological solutions to ensuring the youths e-safety have been attempted, but have not been effective. The solutions aimed to constrain or monitor the users access to the technologies, services and media thereby limiting their allowed range activities. A solution wherein the youth become involved in educating themselves about cybersafety was then outlined as a solution and the focus of the paper’s study. The aim was to “empower learners to develop safe and responsible online behaviours to protect themselves whenever and wherever they go online”(Atkinson et al., 2009). The paper then discusses a research project which evaluated the use of a peer-education initiatives as a way to promote e-safety behaviours and behaviours within UK secondary schools. The conducted study focused on users between the ages of fourteen and sixteen. Eight schools participated in the study. The study involved a two-phase approach. The first phase involved researchers visiting schools to measure the audiences pre-existing levels making use of levels of understanding and
attitudes to online safety and security. They measured this using staff interviews and target audience focus groups and awareness-raising workshops. The second phase was the instatement of student representatives as E-safety Ambassadors within their own schools. In this role, the students were required to champion the e-safety message at their schools. The students worked with the research team to develop or modify their own resources and approaches to delivering the e-safety message. The findings of the study were then presented. Firstly, the dominant threats, as they were perceived by the target audience, were cyberbullying, identity frauds, internet attacks and social networking. Secondly the activities within and results of the e-safety ambassador program were then examined. A key task for the e-safety ambassadors was to promote e-safety messages to their peers. To varied degrees, the ambassadors attempted this by customising awareness material and providing resources to their schools. Examples of these resources included: personalised e-safety websites, videos, posters, display stands, comic strips and assembly presentations; the formation of safety communication forums; and awareness raising activities in specific topic areas. Some of the student ambassadors involved the teachers at their schools in their activities. Overall the study is second phase found that the peer-driven approach significantly impacts the target audiences e-safety base knowledge or awareness. From the start of the study the target audience had already been extremely knowledgeable, in the area of technology and about the need for security when using technology. Therefore, their awareness levels were not significantly improved. However, the peer-driven initiative did have a positive effect on the audience’s actual behaviour. It successfully motivated the learners to modify their actual online behaviour to become more secure. It was noted that the personalization of the awareness approach within each school (the context) was effective and may have contributed to the messages being more readily received than generic awareness-raising exercises.

Aytes and Connolly (2003) present a model which is intended to assist in predicting user’s behaviour in relation to computer security. This research considers the human element of information security. It recognises that human’s play an active role in information security solutions’ However it also recognises that due to user behaviour which may consciously, or unconsciously lack consideration of security, users are frequently a vulnerable component of a security solution. The authors relate how common solution to address the vulnerability created by human-behaviour is the raising of security awareness amongst users about various security threats, and the provision of training to enable users to implement the proper countermeasures to the known threats. The authors acknowledge that these solutions are required, however they argue that is an oversimplified approach to changing and behaviour. They argue that users may not be intrinsically motivated, by the awareness and training, to actually implement the
countermeasures. They state that users may simply choose to not implement the countermeasure even if they are aware of and trained about them. The authors aim to understand why users make such a decision. Behavioural theories which deal choice between risky and safe behaviour are considered. The user’s perception of risk is the focus of this behavioural model. The authors present a model of the factors they believe to impact the user’s decision about their security behaviours. The decision model consists of six components: Information sources, the user’s knowledge, the user’s perceptions, a choice process, the behaviour associated with the choice, and a resulting outcome that then feeds back as a source of new information. Information sources are depicted to feed a user’s knowledge. Information sources include formal training received, news/media, friends and co-workers, policies and procedures and personal experience formal training, news or Media, policies. The user’s knowledge is thus formed about threats and vulnerabilities, awareness of countermeasures, potential consequences to themselves and others, and the costs of secure behaviour. The user’s knowledge affects the user’s perceptions of availability and usability of safe practices, the probability and significance of negative consequences, the ease of recovery and the user’s beliefs regarding peer behaviour. The user’s perception and risk attitude feed into the behavioural choice process. The process results in a behavioural choice (risky or safe) and that choice can have a subsequent outcome. The outcome may be positive or negative, and can provide feedback as part of the information sources. This model presents a continuous, knowledge and behavioural predictive cycle. This paper focuses on predicting behaviour rather than educating users by providing knowledge and changing behaviour. However, its relevance lies in its depiction of what affects the user’s behaviour. Training is considered an information source within the model. Training should take into consideration this model of how users make decisions regarding computer security behaviour, and they should emphasise the points that users consider when they make decisions, e.g. consequences, availability, etc. The importance of taking into consideration lessons learnt from the outcomes of decisions and behaviour as part of personal experience is also an important lesson for the training to adopt. This recommendation can be considered a content recommendation.

Bishop (2000) presents an essay on the different forms of education required to address peoples growing need for information security knowledge and behaviour. The focus is making use of the educational format which is most appropriate for the overall context. The target audience ranges from members of the public to information security experts. The educational streams discussed include information security: awareness, and the academic education formats including training, undergraduate education, terminal master’s education, and doctoral education. Bishop provided
Chapter 3 Information Security and Cybersecurity Education

a discussion of and basic guidelines for each of the educational streams. Public awareness is described primarily procedural form of education. It raises the public’s awareness about information security threats, and what members of the public can do to protect themselves. Comparatively the academic formats offer more in-depth instruction i.e. the “what” to do and the” how” and/or “why” to do it. Bishop states that training focuses on the actions and knowledge needed to react to particular systems or situations, or both. It conveys knowledge on "how" to behave and react. Training is procedural, and the educational format of choice for trade organisations as well as professional and commercial groups. Training is often presented in a hands-on, interactive tutorial and supplemented by slides and added literature material. The interactive approach is considered particularly effective for training individuals. The multifaceted approach of interactive activity combined with documentation was noted to have an enduring effect on the user’s long-term knowledge and behaviour. The undergraduate-, terminal master’s- and doctoral education formats targeted more specialised users who are studying in the field of information security or a related study area. These education formats were not relevant for the purposes of this thesis. Overall, Bishop expresses the view that all forms of information security education should be made use of, and all information and information technology users should be educated. Raising awareness and skills will aid in the protection of the public and general users, while research and higher education will provide subject experts, business executives and management with an understanding of how information security affects their businesses. The research will also provide the material needed to train these information security and business authorities, while increasing the amount of research carried out on information security will result in the establishment of higher education facilities. Thus, ideally a continuous feedback cycle could be created, promoting a subscription of information security awareness, knowledge, and behaviour. Children were never specifically mentioned as part of this papers target audience. However, this thesis can learn and apply lessons learnt from the paper about how to present the different types of cybersecurity education. This source did not explicitly mention children, but it did provide some guidance on what content different levels of education should focus on.

Bryce and Klang (2009) investigated the online behaviour and information disclosure practices of the youth and how their choices and control of this information impacted their online privacy and potential safety. The researchers began by examining the existent range of personal information which can be disclosed by the youth. Then, they identified the associated risk perceptions and disclosure practices for the information amongst the youth within online environments. The authors note that many youths perceive themselves “to have control over their disclosure of personal information online, and do so in full awareness of the associated risks and confidence.
in their ability to manage potentially negative outcomes”. It is suggested this information is done form and maintain online relationships and communication. This intern suggests that “the socially normative nature of online disclosure runs counter to educational strategies”. The authors state that advice for control of disclosure, rather than advice for no information disclosure, should be central to educational strategies which encourage safe and responsible internet activity. Thus, they recommend that education strategies should focus more on encouraging young users to protect their online privacy by being vigilant about disclosing their personal details and by considering potential third-party (commercial and non-commercial) use of their information. The paper finally identified that these education strategies and their content would need to be either selected or designed based on empirical research that explored young people, their online behaviour and the factors that influence this online behaviour. Factors to consider include everyday context, practices, and social norms. This suggests that the strategies should be based off a target audience analysis and designed to be suitable for each particular audience. A call for more empirical research for the development of these types of educational strategies is then made.

Chunying (2010) discusses the need for information security awareness and education for troops studying to join China’s public security active forces. Having identified the need for information security awareness and education the author then addresses strategies for education. The first strategy is to raise the information security and enhance the safety awareness of the troops. This is to be done in the context of e crew ideological mobilization education. The focus of this type of awareness endeavour is to personalise it to the specific crews and grow their awareness of the need information security knowledge and behaviours in relation to their own context and activities. The second strategy involves the creation and implementation of a compulsory information security curriculum for all the students in lower grades. Its purpose is to teach the basic knowledge and skills they require. The final strategy is the establishment of an information security technical personnel security system. Chunying (2010) concludes by stating that the development public security forces course curriculum could be an effective solution. Further work plans intend to incorporate the lessons learnt from recent, current, and future case studies so as to ensure that the course content remained current and relevant. This will result in a continuous feedback, maintenance, and improvement cycle for the education efforts.

Cone, Irvine, Thompson, and Nguyen (2007) report on an interactive video game called CyberCIEGE which is intended to contribute to teaching computer and network security. This game is being used as part of information security awareness and training campaigns. The game
was designed by teams of information security experts, and game design experts. It is described as “a security awareness tool that can support organisational security training objectives while engaging typical users in an engaging security adventure”. The paper provides an overview of common current training and awareness techniques, followed by an overview of CyberCIEGE itself. The game overview presents the major components of the game, as well as information on how it was developed and tested. In brief, CyberCiege presents an engaging virtual world that combines the human and technical factors associated with an IT environment. The game is designed to be highly adaptable, allowing scenarios to be edited or created to be suitable for a wide variety of organisational target audiences with different levels of technical sophistication. The games content teaches information assurance concepts. The level of difficulty for the content included in the game is dependent on the requirements elicitation process which is run on the target audience. The target audience’s technical literacy level was a major consideration in content selection. Based on the suitable level of content, the game presents learners with scenarios which involve security problems. The learners either prevented or reacted to security events and learnt from their subsequent experiences. Overall, the games effectiveness is attributed to the games adaptability for the audience’s needs, its ability to engage the learners and its affordance of the users with the opportunity to gain tacit knowledge by applying concepts in the virtual environment and thereby significantly enhancing understanding of learnt concepts. CyberCIEGE was tested on uniformed and civilian personnel associated with the U.S. Navy, which can be classified as a type or organisational employee. However, the authors note that the game may be suitable for many types of target audiences including general computer users. Currently, the game is successfully being used in several organisations as part of their awareness training programs for general computer users. No empirical evidence is provided to support if the game was more or less effective than a traditional educational approach. Target audience analysis for requirements elicitation and provision of an engaging, interactive, and relatable experience via the game as a platform were the issues of interest in this information security awareness and training paper.

Conklin (2006) presents a study which examined the design and use of a cyber defence competition as part of an information security curriculum. The purpose of the paper was exploring issues associated with an information security management curriculum and how to effectively develop skills required in the professional career field. The context of the study is the information security management curriculum for graduate students at the University of Texas in San Antonio (UTSA) i.e. future information security management professionals (organisational users). The curriculum and competition content covered the introductory concepts and principles of
information security, incident response, digital forensics, security policies, access controls and security assessments. The depth and difficulty of the curriculum’s and competition’s content was beyond what this thesis would need for school learners. However, the implementation of the course as of interest. The curriculum consisted of three courses, which involve lectures, and limited lab components, and then a fourth assessment class, which involved considerable amounts of practical work and lab exercises. The argument is made that another component was needed in this curriculum in order provide learners with the opportunity to become actively involved in the learning process, and gain practical experience. The logic for this decision is accredited to the subscription to the pedagogy of active learning theory. Active learning, as described by the paper, is a means of delivering content using hands-on activities that involve the student directly in the learning process. The competition provided students with an opportunity to apply their learnt skills and develop team-based management skills in an “operational business environment”. Thus, it provided them with “practical experience” which enabled them to better understand what they had learnt while identifying what they still need to learn. The results of the competition allowed the instructors of the curriculum to evaluate the thoroughness of their curriculum based on whether their students were had the knowledge and skills to respond to the scenario. The competition itself consisted of business scenarios which included realistic event-driven activities to test student abilities and to provide an educational test-bed to encourage growth and collaborative teamwork. The collaborative component of the competition was another pedagogical decision made in the competition’s design. It was based on the premise that interactive components in activities that force interaction with others as part of the learning experience increases the effectiveness of the class in developing student skills. Data was gathered via exit surveys from the competitions participants and instructors. Analysis of the data allowed the researchers to evaluate what improvements the curriculum required, and how the competition participants perceived the competition as a learning experience. The results of the survey showed that all the participating parties had felt that their preparation for the competition experience needed to be honed. Additionally, participants found that the competition, as an active learning exercise, had provided them with much desired opportunities to enhance their education. These results served as provide empirical proof that this approach is perceived to be effective by the participants and instructors. The study shows that pedagogical design of a learning experience is beneficial and practical experiences allow students to grow their understanding of their field of study. It also shows lessons learnt from the experience should be used as feedback motivating improvements to the existing curriculum. These lessons were to be incorporated into the thesis’s practical component.
De Lange and Von Solms (2012) present an e-Safety framework that was developed to raise awareness and increase e-Safety education in South African schools and contribute towards the development of an e-Safety culture. The authors recognise and have inferred that the implementation of e-Safety should be considered essential in the lives of children. However, there is currently a lack of e-Safety education in South African schools. The framework aims to address the lack. The focus is primarily on learners from primary and secondary schools. The authors present a high-level framework which details how proper governance must be in place; the relevant role players must be identified; effective e-Safety topics must be identified; and resources using the content should be identified; and when and where the e-Safety messages must be delivered. This framework is very high level, sowing a view of the process rather than the detailed implementation. It would however e good guidance for integrating cybersafety education into existing school curriculums. The framework is only conceptually presented and validated, it has not been implementation. This thesis will however take into consideration lessons learnt from this paper.

Da Veiga (2015) proposes “a unique information security training and awareness approach (ISTAAP) that can be used to instil an information security-positive culture which will assist in addressing the risk that human behaviour poses to the protection of information”. ISTAAP is intended to be deployed to focus information security training and awareness efforts. it incorporates an information security culture assessment as a core element to direct training and awareness. ISTAAP was developed for organisational use. The paper includes empirical data to illustrate the value of ISTAAP. The model could be used to influence, content, presentation, and delivery decisions in an education effort.

Davinson and Sillence (2010) presented a study which aimed to determine whether users could be encouraged to behave more securely online, through a combination of increased awareness and training. The study was particular relevant to when users were conducting financial transactions online. The authors ultimate goal for this study was to promote secure behaviour amongst all internet users. The paper begins with a discussion of the increased use of the internet amongst users worldwide, and the related increase in online threats targeting these users. Financial transactions are a frequent activity online. A prominent threat that targets these the information and users of these transactions are phishing attacks. The risks of falling victim to such an attack are outlined. Thus, the authors looked at what solutions were available for addressing the issue. It was stated that there are several technological precautions and defences which can be taken against phishing, however the authors believe that the targeted users also need greater
awareness and training for identifying and defending these attacks. It was stated that in order to modify a user’s behaviour, they would require the relevant knowledge and the motivation to behave in the desired manner. In relevance to online activity, existing literature showed that users have concerns about the security and privacy of the data which they provide to websites during financial transactions, however they were simultaneously willing to compromise this data for in exchange for perceived “benefit” (convenience, affordability, access etc.) gained from a transaction when they considered it credible. Thus, users have a conflict in their relevant security attitudes and behaviours A user’s ability to evaluate the credibility of the online transaction, and the subsequent behaviour pattern of a user, is influenced by their knowledge and motivation. Thus, in order to modify the user’s behaviour, these areas need to be addressed. The authors aimed to address this by following an adapted version of a psychology model called “The Health Belief Model (HBM)”. The authors explain the model and outline how the study aimed to address the knowledge and motivation issues using two methods. The first method was educating users via a training program, thereby providing them with the necessary knowledge. The second method was the manipulation of risk levels, to increase the user’s motivation as a result of the perceived susceptibility to the threat. The effects of both methods were tested by analysing subsequent self-reported behaviour of the studies participants after exposure to either method. The chosen two methods were based on meeting the plan of an adapted version. The authors then discuss an experiment they conducted using an interactive computer game known as “Anti-Phishing Phil” as part of an educational training program. The experiment, its design, and the participants the study were then discussed. In a brief summary of what was covered, this training programme informed users of the common types of phishing threats and how to identify them. During this process, risk level manipulation randomly allocated the categorising of the participants in the experiment into having the potential to be either a high risk or a low risk victim of online fraud. The experiment found that offering a “tailored” or seemingly personalised notification to users, regardless of their perceived risk level, increased the users’ intentions of behaving in a more secure way online. Personalisation is thus a key issue covered within this study. Conversely, it was found that the training programme had no effect on the users’ secure behaviour in general. Due to the target audience of this study, the type of security this study dealt with was cybersecurity. The objective of the study was not explicitly linked to the fostering of a cybersecurity culture, however it dealt with the underlying component of knowledge and behaviour using awareness and training activities.

Desman (2003) authored an article about the ten tips he prescribes as the unofficial “Ten Commandments of Information Security Awareness Training”. The purpose of these
Chapter 3 Information Security and Cybersecurity Education

commandments is to provide some basic guidance for information security personnel to use when trying to communicate the importance of information security practices to other users within an organisation. Enabling communication with the majority of the target audience, and successfully make them aware of the general importance of information security, and the its relevance to themselves and their activities is the commandments ultimate goal. The advice which can be abstracted from the commandments will be briefly summarised. Commandment one emphasized the importance of people in information security training. Humans play an essential role in information security and need to be aware of all their roles and responsibilities. Communicating with the users is stated to be the most important part of an information security system. The second commandment stresses that communication should be understand and relatable. Therefore, language, jargon and explanations should be aligned with what the user will understand. The third commandment emphasises that multiple methods of communications channels should be used to spread the message in order to reach the entirety of the audience. The fourth commandment recommends ensuring that the message and purpose of any awareness effort are clear to both the designer and the receiver. The fifth commandment recommends making the message as readable and enjoyable (in the context) as possible, so as to prevent indifference from the target audience. The use of appropriate humour is a suggested example of achieving this “sugar-coated” version of a message. The fifth commandment recommend conciseness in communications while keeping them informative. This is recommended in order to avoid “information overload”, but ensure that the information which needs shared is communicated and understood. The seventh commandment recommends that it be made clear to the audience how the requested information security behaviours would affect them. The eighth commandment recommends making use of existent resources, e.g. communication channels and personnel, within your campaign in order to gain the benefit of their experience, and abilities for your own campaign. The ninth commandment recommends the formalisation of the training methodology. This formalisation includes a renewable security agreement, constant “refresher” courses and educational media resources, and a security presence to be maintained among the users. Finally, the tenth commandment involves maintaining and ensuring that awareness efforts, material and topics are both recent and relevant. This recommendation also encourages the inclusion of content from the media and other sources. Overall this paper dealt with an overview of how to design an awareness training approach without provide explicit guidelines. Lessons to be learnt from this article included the importance of the relationship between the target audience and included content within overall course approach, and the advice of re-using existing resources
Dodge, Carver, and Ferguson (2007) conducted an unannounced security exercise with users who had been previously exposed to their information assurance education program. The exercise involved phishing-styled emails being sent to the learners to test their awareness of the threat after exposure to the course. Four types of e-mails were used. The first type of e-mail asked the student to click on an embedded HTML-encoded link. The second was identical to the first but asked the student to open a .html attachment. The third e-mail, asked students to click on a link which took them to a site which asked for sensitive information. The fourth e-mail asked the students to follow a link to download an application and run the application. This exercise served to firstly re-enforce the knowledge that the learners had learnt, and secondly aid in evaluating the effect the phishing aspect of the education program. The exercise as repeated multiple times over a few years. Results from the exercise were used to improve an existing information awareness programme. The overall finding of the exercise was that many of the learners “fell victim” to the phishing email. This meant that the learners continued to unintentionally disclose information to unknown third-parties, and “expose themselves to malicious code by opening attachments”. The type of “unannounced” testing of the effect that the education program had had on the users could be adapted and used in other training programs. The results serve as a measurement of the curriculum’s success without the biases that may have affected such a test if the users had been aware of its occurrence and their participation. This method can be used as part of the feedback process of a campaigns maintenance. Lessons can be learnt regarding content selection in particular. Overall this campaign aimed at testing knowledge by testing behaviour.

Du, Shang, and Xu (2006) examine the use of the use of laboratory exercises as part of computer security education courses at universities. These courses are targeted at future computer information security professionals. The authors make the argument that pedagogical research has shown that practical exercises and hands-on experiences (“learning by doing”) are critically important to the success of this type course. Exercises provide the students with the opportunity to re-enforce learnt knowledge by apply what they have learnt. The authors describe a variety of approaches for the design and implementation of laboratory exercises. The authors opted for an instructional approach. This approach involves providing the students with access to a courseware system which serves as an experimental platform and framework for computer security courses. The system contained a number of projects for helping students focus on: grasping security concepts, principles, and technologies; practicing design and implementation of security mechanisms and policies; and analysing and testing a system. The authors discuss the design choices made for their “laboratory. It is designed using Minix OS. The authors designed their lab exercise to allow the students to focus on one, or a select few, principles during each
exercise. A detailed overview of the security concepts to be learnt is then also provided. Finally, a discussion of the experimental laboratory exercise experience is provided (content). The response of the students to this type of exercise was positive. The experience was evaluated as being engaging and encouraging for students. Overall this paper can be used as a guideline for designing and implementing a simulated practice exercise to teach and reinforce security knowledge and behaviour of future IT professionals.

Eminağaoğlu, Uçar, and Eren (2009) present a case study of the implementation and evaluation of an information security awareness training program. The paper begins by explaining that information security awareness training is an important part of addressing the human aspect of information security management. The paper begins by briefly outlining information security management, and the need to address the human aspects of the practice. Exposure of users to proper awareness education and other awareness materials or tools on a regular basis, is identified as one way of dealing with this issue. Based on this premise, and motivated by a few security breaches which had occurred, an education program was conducted as part of a case study. The case study presented in this paper describes an information security awareness campaign which was conducted at a Turkish company. The goal of the campaign was to raise user’s awareness of security issues relating to password usage, password quality and compliance of employees with the password policies of the company. 2900 employees were exposed to the programme. The campaign consisted of formal training (implemented via lectures and training sessions), and other supplementary awareness campaigns such as educational posters, animations and e-messages on the company Intranet, surveys, and simple online quizzes. During the campaigns implementation time three password security strength audits were conducted. Based on the finding of the audits, the awareness training and other related campaigns had positively changed the user’s password related behaviour. The audits found that weak password usage had decreased, employees had become more aware of security on an ongoing basis, users had increased their participation in security efforts and more employees had begun to comply with the company’s information security policies. The researchers, thus, concluded that education and awareness are one of the most effective and powerful mechanisms for mitigating information security risks. They did, however, note that efforts should be continuously supplemented with supporting materials. It was of particular interest that they noted that the materials provided should be customised to suit the target audience and that they must be both user-friendly and attractive to employees. User motivation and usability of the training materials were identified as critical success factors of the programmes. Eminağaoğlu, et al. (2009) also recommend ensuring that the material is enjoyable and motivational rather than tedious. The use of visual materials which
were designed by experts and shared concise messages were recommended. This paper can be consulted for basic guidance on how to present content.

Endicott-Popovsky, Orton, Bailey, and Frincke (2005) discuss a security awareness event which was designed to raise awareness among a community’s leadership of the vulnerabilities of data held in private and public databases to Internet attacks, particularly identity theft via Google hacking. The authors begin by describing the standards for the development and implementation of security awareness training described in NIST Special Publication 800-50. NIST800-50 recommended that all users of any information system be made aware of their roles and responsibilities in maintaining security. To achieve this, it recommends exposure to awareness campaigns and events. Guidelines for such event suggest that events should be customised to suit the intended audience, the message being delivered and the desired outcomes while simultaneously gaining the attention of the target audience. The authors discuss an event which followed these guidelines. The relevant event was a Google-hacking contest, which was run in Seattle, Washington, by Agora forum. The main educational objective of the event was to make local community and business leaders aware of the need to protect the information contained in the databases of their organisations due to the vulnerabilities of networked systems to Google-hacking’. The secondary objective was to inspire related legislative change. The need for this particular subject-matter was attributed to common security malpractice or negligence in the subject area, and to the associate poor organisational culture surrounding the issue. A full explanation of the competition’s rules and implementation was provided. It emerged from the results that the winners of the event had identified more than one hundred million potential opportunities for identity theft. This finding drew both local and national attention and resulted in discussions about possible state legislative reforms. The researchers concluded that a security awareness programme, based on NIST standards, may be effective, not only for organisations but also for specifically defined communities. Overall, this initiative did not encompass a traditional educational approach. However, the initiative did comply with the “attention grabbing” requirement of NIST. The events purpose was to raise community leaders and the general public’s awareness of information security issues relating to their information on networks, however it also served as an educational tool for future information security experts. The practical experience served as an effective teaching tool for the participants (mainly university learners in the field of information security). Overall the competition was effective at raising awareness amongst its target audience, and at educating the involved learners and other participants.
Furnell (2008) examines the growing need of end-users, throughout society, to adopt a security culture. The author has identified that online service adoption has been vast and rapid, and related threats have increased, however end-users have not adopted related security knowledge and behaviour. End-users are therefore not conducting online activities securely, and they are taking unhindered risks. All end-users to bear some responsibility for securing their information and activities, however because they lack security awareness or are not motivated to behave securely most users do not fulfil this role. Multiple case studies are cited as proof that users engage in risky behaviour. Examples of such behaviour included accepting unknown people into their online friendships. The cases also showed that all age groups (adults and youth) lack security awareness. This state of affairs indicates that there is a need for security and privacy awareness. The author argues that it is essential that society develop an information security culture. Education and awareness were identified as a starting point for fostering such a culture, as it provides users with the requisite security knowledge. The author states that freely accessible awareness and advisory sites are already available, however to reach their target audience, it is necessary to first attract the user’s attention. Current methods are not particularly effective at fathering attention. A call is made for more channels of communication (delivery) to be used to actively push security messages to relevant user communities in both domestic and workplace contexts.

Furnell, Gennatou and Dowland. (2002) describe a prototype implementation of a software tool that allows self-paced information security training. This educational tool was developed in an attempt to address the need information security awareness within small organisations. The paper begins by outlining the need for comprehensive security solutions in organisations. The need for staff to be aware of and behave in accordance with security policies and procedures is highlighted. A need for appropriate information security training and awareness which teaches appropriate knowledge and behaviours in order to help establish an information security culture is identified. This paper focuses the need for these educational efforts in small organisation which have less than a hundred employees. The reasons for focusing in this context are briefly outlined. Issues which affect the implementation of awareness efforts in small organisations are then briefly discussed. Identified issues include lack of security staff, and limited financial resources for an awareness effort, lack of risk perception and a prioritization of other business priorities over security. Furnell et al. (2002) argue that a computer-based training (CBT) solution for information security awareness and training may be an effective for the users within smaller organisations. A security CBT training tool which enables users to test their understanding of information security principles and behaviours is then described. The tool’s purpose is to individuals to complete self-
paced security training the prototype software tool is described as providing an interactive, user-friendly learning experience. The training involves simulations of several predefined case-study security scenarios. The aim of such training is to teach the staff undergoing the training course what security countermeasures are available and how to react in the context of specific scenarios. The training aims to provide the learner with the realistic cognitive experience to assist their understanding of taught or learnt concepts. The material was presented as a scenario and included both a picture and relevant information. The scenario picture allowed exploration via clicking of the highlighted areas. Overall the presentation comprised an interactive design which encouraged exploration and interaction with the "scenario" and engaged the learner. The proposed tool is adaptable to multiple contexts, as it allows the users to also define new scenarios and content as necessary. No empirical evidence about the effectiveness of the presented tool is provided. This paper provided some recommendations on how to deliver materials, and how to present it as an interactive experience using a technological education solution.

Futcher, Schroder, and Von Solms (2010) examined existing approaches to education in information security. They also conducted a survey to establish the extent to which information security is currently incorporated into the IT/IS/CS curricula at South African universities. They identified that students and IT users and future information security professionals (at organisations) require exposure to information security awareness and education. The paper briefly discussed outcome-based education with a specific focus on broad learning competencies. This was followed by an examination of critical cross-fields outcomes. The paper then proposed to meet the students’ need for information security education by explicitly defining information security as a critical cross-field outcome (CCFO) within university programmes. It was hoped that this would result in information security aspects being integrated into various learning programmes. According to Futcher et al.(2010), this would be particularly helpful in addressing the “information security gap” that currently exists in IT/IS/CS undergraduate curricula at South African universities. The paper provides a table of information security topics which are either found or may be included in information security courses. However Futcher et al. (2010) cautioned that the selection of the content would depend on the particular needs of the students concerned.

Goucher (2008) briefly highlights and explains common mistakes that are made in information security awareness training targeting organisational users. The argument was put forward to engage non-traditional training methods and techniques so as to engage and hold the attention and interest of target audiences. The common mistakes listed include the running of long, expensive training sessions, confusing a lack of enthusiasm for the security awareness training
with resistance to security awareness, irrelevant (or out of context) security training, inappropriate or overly technical training and the inclusion of too many people in a single training session. Goucher did not provide a definite conclusion as to how to present and deliver material. But Goucher did indicate that presentation was important and that it contributed to how understandable the material may be for the users. Delivery channels such as online material, real-world classes and multimedia were suggested as possibilities.

Goucher (2009) identifies various challenges that may be encountered during the implementation of security awareness training targeting organisational users. The most prominent of these challenges is the continued use of outdated educational approaches in order to teach information security. Goucher makes a number of recommendations about ways in which to overcome the various challenges. The first recommendation involves ensuring that a course is both developed and presented well as the more engaging a course, the more effective it may be. The second recommendation involves making sure that purpose of the course is effectively and efficiently realised. This includes ensuring that the material is topic specific, relevant to the course objectives and time effective. It is emphasised that a successful course encompasses three important elements, namely, attention (presentation and delivery of the material to gain the learners’ interest and to promote understanding), retention (encouragement of retention through procedural learning and repetition) and motivation (motivating the learner to engage and participate). These factors and issues which are considered the current challenges of information security training approaches all emphasise the need to teach information security awareness in such a way as to help the learners to understand the concepts.

Grimson, Grimson, Flahive, Foley, O’Moore, Nolan, et al. (2000) presented a multimedia-rich information security and communications technology awareness programme targeting health professionals in Ireland (organisational users). The material was delivered via a symposium and supported by a CD and associated website. The paper highlighted the advantages both of multimedia in presenting material and of e-learning technologies as a convenient, accessible delivery mechanism. The content was applicable mainly to the way in which ICT may be effectively integrated into all healthcare sectors. Although information security was not the focus of the article it was incorporated into the general user education programmes from the beginning.

Hagen and Albrechtsen (2009) measured and discussed the effects of an e-learning tool aimed at improving the information security knowledge, awareness, and behaviour of employees. This e-learning tool was presented as a large-scale, computer-based, and standardised security training effort. Empirical evidence regarding the effectiveness of the e-learning based information
security campaign was presented. The study documented and compared pre- and post-training assessments of employee knowledge of information security, as well as employee attitudes towards information security. A theoretical model was provided to show how specific content had been chosen to be presented to an employee. This choice was designed specifically to meet the material need of influencing employee behaviour and was based on the employee’s current attitudes and knowledge. No guidelines were provided to aid in the selection of what information security awareness content should be included. Nevertheless, the following modules were included in the material, namely, Introduction to Security, Information Security, Travel Security, Personal Security, Security of Facilities, and Internal/External Communication. Although one module only focused exclusively on information security, information security was integrated into and included in the other modules as well. These content categories could be applied to other programmes. The material was delivered via interactive e-learning software while, from a presentation perspective the material was presented using vocal instructions, pictures, music, and text. The material was presented in scenario and problem-based formats, including exercises, tests, and feedback. This model was followed by the design and results of the empirical experiment itself as shown by the findings presented. The study’s findings indicated that there was a significant short-term improvement in the information security knowledge, awareness and behaviour of those individuals who were part of the intervention group. Although the study had focused on the short-term effects of the course it did propose that future work be carried out to measure the long-term effects of the course. It was then stated that e-learning programmes, such as this individual information security awareness training, could be used as an initial starting step in the development of an information security conscious corporate culture.

Hagen, Albrechtsen, and Johnsen (2011) continued the research they had started in their 2009 paper. The purpose of this paper was to measure and discuss the long-term effects of an e-learning tool aiming at improving the information security knowledge, awareness, and behaviour of employees. The research determined that not all the short-term effects of the e-learning awareness programme translated into long-term effects on the knowledge, awareness, and behaviour of the target audience although some of the effects did last. Thus, a need for recurrent training, on an annual basis, was identified as a prerequisite to sustaining the effects and thereby ensuring that the short-term information security knowledge, awareness, and behaviour did not diminish.

Hentea (2005) discussed issues in information security awareness education which required changes if they were to be resolved. The article begins by discussing the need for an information
security culture in all aspects of information systems and information networks and amongst all organisational and home users. In addition, it highlights how essential it is that users are made aware of this need and also the current absence of the requisite awareness. The paper then examined a possible reason for this need for awareness by highlighting several issues in current information security awareness programmes. Many tertiary education institutions have instituted courses or specialised programmes to teach information security skills to students enrolled in computer-related degrees and it is issues in these programmes that are highlighted. There are many such issues. Firstly, it is vital that information and computer security be taught early on in an educational model with the best approach thus being to educate individuals at an early age. In addition, it is recommended that this computer security education be integrated into other components of information technology education. Secondly, information security should be made a compulsory course instead of an optional extra. Thirdly, audiences beyond immediate learners also need to be educated. In other words, there is a need for all information technology users and IT professionals to be educated as well as for ongoing information security education revision. Fourthly, a standard integration method is needed for the integration of information security topics and other computing topics. Lastly, there is a need in industry for security professionals who are capable of continuously acquiring information security skills and problem-solving abilities and also improving these skills and abilities. This is particularly important in view of the fact that information security skills have been identified as a critical skill within the workforce. In addition, changes in information security disciplines need to be identified and integrated into curricula. Having identified the above issues, the author then suggested possible guidelines for solutions that could aid in solving these issues. It is essential that both IT and non-IT professionals and future graduates be made aware of information security. The notion of including, at the very least, an introductory information security course covering information security fundamentals in the first year of every course at every tertiary education institution is proposed. This course proposal is accompanied by recommended content topics. This list of recommended topics was later supported by a description of the list of security concepts which were included in the undergraduate computer science curriculum offered at the University of Maryland, Baltimore County.

Hentea et al. (2006) discuss information security awareness (ISA) education and course approaches for undergraduates studying to become future security professionals. The discussion includes changes to the course approaches, topics, resources, and the courses themselves. The discussion began with an overview of information security education and the various qualifications offered in the information security field. The differences between professional and vendor
certification as opposed to academic qualifications were highlighted with the academic qualification being cited as being extremely important. Hentea et al. (2006) then discussed the topic of information security education in the US. This discussion covered the various national and international standard creating organisations. Each one was named and briefly elaborated upon while their effects on current university education efforts were highlighted. It was then mentioned that ISA programmes in countries outside the US tend to be characterised by greater variety and flexibility than those within the US. This was followed by an examination of information security curriculum issues, including content, didactic methodology and degrees in Information Security. It would appear that the curriculum issues stem from the overabundance of education and models which have originated as a result of guidelines, such as those provided by the ACM, and which fail to specify the topics, courses, or sequence of courses in an educational context. In an attempt to address these issues, the process of implementing of an effective ISA curriculum based on the curriculum content, methodology, and research was then discussed. Finally, Hentea et al. (2006) suggest actions which may render the ISA curricula in universities responsive to the needs of both the general population and the industries in which graduates with ISA skills and specialisation will be employed. These proposed changes included suggesting that information security education include both technical and nontechnical content; that the content is kept up to date as required by the public, industry, and government; that the curricula include courses and experiments which encompass Intelligent Systems and Artificial Intelligence techniques that support the intelligent control of security and create a knowledge base for the information security domain, that students in computing disciplines learn how to develop information security tools and scholarly research be undertaken exploring new technologies and new approaches designed to find more effective and long-term security solutions. Hentea et al. (2006) suggest that the curriculum content of an information security assurance programme must be multidisciplinary with inter-related topics the fields of computer science, computer engineering, mathematics, management, information systems, business, political science, psychology, sociology, and law. Hentea et al. (2006) suggest the educational experience use pedagogical tools, based on simulations that support interactive step-by-step demonstrations of the protocols, processes and algorithms aimed at facilitating the students’ learning.

Hu and Meinel (2004) presented an e-learning information security training approach targeting IT students and professionals. This approach targeted IT students and professionals. The objective of the e-learning programme was to provide an isolated environment in which learners were able to experience simulations of security situations and thereby gain hands-on experience as well as being exposed to tutorials. All the tools required to complete the exercises were provided on a
CD. The content of the course was extremely technical in its focus. According to Hu and Meinel (2004), there were, at that stage, five chapters available. These chapters dealt with cryptography, digital certificates, secure email, authentication, and access control. It may be assumed that these topics and a few others could be included in other technically focused information security training courses. The material was delivered via a CD and it was presented as a virtual laboratory environment. The material was presented as interactive security exercises. By example it would appear that this material advocated e-learning and technological delivery for information security material.

Johnson (2006) identified that it is critical that information and IT users be aware of and follow appropriate information security guidelines as it is a recognised fact that people often constitute the weakest security leak. Accordingly, this paper advocates that every effort be made to ensure that all users behave in a secure way. But the paper was presented from an organisational perspective. This would include the implementation of an information security solution, especially of the awareness, training, and education components of such a solution. Within companies Johnson (2006) recommended that information security professionals work to gain space on the board’s agenda by focusing on the organisations focal business issues and providing information on related business benefits, risks and benchmarks. They are then urged to emphasise the need for information security, explain the reasons why it is necessary and, through the use metric measurements, illustrate how the business may benefit, for example, through the return on investment potential. It is hoped that, in this way, the information security professionals would be able to convince the corporate users to make information security and its implementation a priority.

Johnson (2006) also highlights the various costs and benefits of a security awareness programme as part of its implementation. The rest of the paper addressed information security awareness and education programmes with specific focus on the development of information security awareness course material. The paper stressed that all departments within an organisation should be involved in the security effort and also in the development of the security material. The paper provided examples of the various skills which certain organisational departments could contribute to the content selection, and presentation of the course material. The paper also addressed the selection of topics to be included in the course. It was suggested that certain topics be compulsory while others could be optional. The paper noted that the various topics would be targeted at different or multiple audiences. It also indicated that topic levels should be prioritised based on the organisation itself and its business or service objectives. Finally, the paper discussed the
matter of the presentation and delivery of the course material and how it could be used to enhance the effectiveness of the course. Several promotional, informational, educational/interactive and enforcement methods were suggested for the presentation, navigation, and delivery of the information security awareness material. These recommendations included technological and non-technical presentation and delivery formats. The rest of the paper then re-emphasised the importance of integrating information security into all business activities.

Katsikas (2000) discussed a methodology for identifying the information systems security training needs of personnel classes in health care institutions. The paper begins by providing background information about the integration of information technology and networks into health care systems. These systems have become known as health information systems (HISs) and there is a high degree of dependence on them. This dependence has, in turn, led to security risks and it is for this reason that this paper provides the information security education methodology designed to render the user aware of these risks. The educational methodology classifies security education into three sub-components, namely, awareness, training, and education. Each component is delineated by differences in the degree of comprehension and detail. The cybersecurity education process begins with awareness and progresses through the other two components, each building upon the knowledge acquired in the preceding component.

Having established the structure of the information security education methodology, Katsikas (2000) then examined the body of knowledge to be incorporated in the appropriate components of the methodology. The information security training content was also organised into three categories. These categories included content related to the legal, regulatory, and ethical frameworks relevant to information systems security; content related to information systems security policies and content related to information systems security controls. Finally, the paper concludes by examining a current security awareness education programme (ISHTAR) which was already in use in the health care environment. The programme was evaluated against the derived learning needs of the specific target audience. In the main, it was found that the course was adequate. Nevertheless, a few content issues were highlighted. These issues included the course material not acknowledging managers as information systems users; the ISHTAR course depriving managers of their role as the acquirers of information and the course failing to cover the training requirements adequately as a result of the fact that managers may be called upon to manage both security management controls and training and awareness controls.

Kritzinger and Smith (2008) proposed a conceptual, multidimensional Information Security Retrieval and Awareness (ISRA) model. This model was intended for use in industry and it aimed
to enhance the level of information security awareness amongst employees. The first “building block” of the proposed model comprises a collection of national and international information security documentation, including standards, best practices, etc. The second “building block” of the proposed model comprises a large common body of knowledge about information security which is suitable for industry use. The proposed common body of knowledge is divided into technical information security issues and non-technical information security issues. The third building block of the model comprises the IT authority levels. These authority levels consist of stakeholders who are responsible for ensuring the survival of an organisation. In the model, the stakeholders are grouped together according to their job categories. The first three “building blocks” comprise the first dimension of the three-part model, with this dimension addressing non-technical information security issues, IT authority levels and state of the art information security documentation. The second dimension of the mode focuses primarily on retrieving relevant information from the ISRA components of the first dimension. This information is then used to enhance the level of information security awareness at all the IT authority levels as well as to assist IT authority levels in decision-making processes. This second dimension is known as the information security retrieval and awareness dimension. Finally, the third dimension of the model consists of methods for measuring and monitoring the current information security awareness status within an organisation. This dimension helps to ensure that all new information security issues are incorporated and addressed in the common body of knowledge. In short, the proposed model consists of the following three components, namely, the ISRA dimensions (non-technical information security issues, IT authority levels and information security documents), information security retrieval and awareness and measuring and monitoring. It is important to note that the model focuses specifically on the non-technical information security aspects of the common body of knowledge. Lessons learned from this paper relate to the different of content covered.

Kritzinger and Von Solms (2010a) investigated the information security awareness state of home users and proposed an awareness model which was aimed at increasing the awareness of this group of users. The paper began by discussing personal internet users. These users have become increasingly exposed to security threats and, in addition, they are often particularly vulnerable to the effects of these threats. This vulnerability stems from a lack of the knowledge and skills required to secure themselves against these threats although this varies for the various types of personal internet users. Kritzinger and Von Solms (2010a) provide a differentiating classification of these types of users by categorising the users as either non-home users (NHUs) or home users (HUs). It is further explained that NHUs often obtain vital information security knowledge through their working environments as opposed to HUs who do not. Kritzinger and
Von Solms (2010a) define a HU as a "citizen of varying age and technical knowledge who uses Information Communication Technologies (ICTs) for personal use anywhere outside their work environments" and "who is self-responsible to secure that computer in terms of malware, updates, patches etc." It is then re-emphasised that these users are not obliged to obtain information security knowledge in any form, with this lack of knowledge resulting in their being especially vulnerable to cyber threats. The authors of the paper believe that one of the main reasons for this lack of information security awareness on the part of HUs is the fact that there is no third-party enforcing HUs to use the Internet in a secure way. Clearly, it is essential that this situation be rectified.

Their argument is then supported by a brief comparative overview of information security awareness efforts for non-home users as compared to home users. It is blatantly obvious that there are several approaches and educational approaches available for NHUs but few for HUs. However, the few education programmes which do target HUs have identified several issues including the fact that, in general, online programmes are hard to find, the content covered is not comprehensive enough, the content usually provides limited information which is suitable for beginners, there is no dynamic interaction with the users by means of testing, examples and exercises and, finally, the programmes are not updated on a regular basis with new, emerging technologies. Accordingly, Kritzinger and Von Solms (2010a) proposed a model that would, firstly, provide a framework for the design and implementation of information security awareness tools suitable for HUs and their varied skills levels and, secondly, provide a way to force HUs to be exposed to these tools for their own education and benefit. This proposed model is known as the "the E-Awareness Model (E-AM)". The aim of the model is to force users to become aware of and familiar with the risks associated with cyber activities by presenting some information security content and forcing the users to absorb this content. This process is supported and explained by the model.

The model comprises the following two components, namely, an awareness component and an enforcement component. The awareness component is found in the E-Awareness Portal. The function of this component is to provide up to date content regarding information security risks within the home user environment while the enforcement component is addressed by hosting the E-AP in the context of certain regulating services. The function of these regulating services was to ensure that access to the Internet became possible only after the awareness content aspect in the E-AP had been passed. The paper did not expand on precisely how the ISP would manage and control the levels in the E-AP to which the user would be exposed or when the user would be
exposed to these levels. However, Kritzinger and Von Solms (2010a) did acknowledge this to be an implementation issue.

Kritzinger (2015) attempt to address South Africa’s lack of initiatives to ensure cybersafety among school children. It does this by proposing the concept of cybersafety games that can be distributed to schools and translated into different languages. The paper focuses on determining what the current status of cybersafety is in developing countries, and how gaming be used to bridge the educational barriers that exist in developing countries to enhance cybersafety among school children. A cyber-safety framework that incorporates all the necessary design inputs create an offline game that can contribute to the cybersafety awareness process in South Africa. The paper did not provide presentation or delivery methods beyond the recommendation of developing offline games. However, it did recommended topics. A meta-analysis keyword search. Was conducted with three identifiers: environment, users, and actions. Topics were presented in relation to cyber risks and cyber countermeasures.

Kruger and Kearney (2008) investigated the application of two management science methodologies to the problem of identifying the most important areas to be included in an Information and Communications Technology (ICT) security awareness programme. This program targeted all computer users in a mining organisation. Their aim was to obtain consensus rankings from the various role players regarding the higher or lower priority status for inclusion in information security awareness programmes of the various components. The first methodology was described as being based on the concept of minimising the discrepancy between individual rankings through the solving of a linear assignment problem while the second methodology was based on a heuristic approach known as the maximise agreement heuristic (MAH) approach. These methodologies were presented in relation to a real-life case study from the mining industry. A simple questionnaire was used to gather data and obtain the awareness rankings in terms of priority. This technique provided a better understanding of the relative importance of specific factors influencing the information security awareness programme and saved time and money for the process. The application of the techniques described in the paper may assist in identifying and prioritising improvement opportunities in an easy and transparent way while also enabling decision makers to address the security awareness problems in any area associated with ICT security in an accurate way.

The selection of content was the focus of this paper. The content was selected based on careful deliberation and a risk elimination process. It included the following six focus areas, namely, company policy compliance, password management, e-mail and Internet use, mobile equipment
security, incident handling and general awareness. The programme was presented in multiple languages using video presentations, personal presentations, a website on the company's intranet, brochures, posters in offices, and articles in the company’s in-house magazine.

Näf and Basin (2008) focused on the importance of hands-on, interactive, and individual course work in information security education. Such an approach increases the understanding and retention of theoretical work while also helping the learners to apply what they have learnt in reality. The paper examined the way in which laboratory-based courses in information security could be designed. It examined both the conflict-based and review-based approaches. Both of the approaches were proven to be acceptable and effective in encouraging engagement in the experience and retention of the material. Combining these advantages was also suggested as a potential approach which may have several benefits although it would require considerable time and resources to be completely effective. This research did not specifically identify who the course targeted or what content to include in the course.

May (2008) discussed seven pointers for the development of an effective, relevant, attractive, and well-presented information security awareness programme. The first pointer involves "making it personal". This pointer is based on the premise that people relate best to issues which affect their own interests and circumstances and, thus, it is recommended that information security messages be presented in a context to which staff members are able to identify and which they understand. The second pointer involves "matching the message to the audience". In other words, the technical level of detail presented should be based on the skill range and level of the target audience and, thus, different training material would be needed for different audiences. The third pointer involves "keeping it short" as the presentation of brief, meaningful messages was more likely to be effectively remembered than a lengthy document. In addition, brief presentations are also less likely to induce boredom and disinterest. The fourth pointer involves "making it interesting". In other words, explain, provide examples, and use humour to convey and communicate the message which may, otherwise, be considered staid and be easily forgotten. The fifth pointer involves "using real-life examples". Real-life examples may be extremely effective in demonstrating what may otherwise have been considered as theory only. The sixth pointer involves "making it part of everyday business". If the topic is interesting and well-presented most staff members will participate in the training readily, particularly as it gives them a break from their daily routine. Inserting security messages in everyday business may subliminally aid in the subconscious creation of a security culture within an organisation. The seventh and final pointer involves "using the right delivery method". Once again, the delivery and presentation methods
should be selected based on the needs and preferences of the target audience. Lessons learned from this paper indicate that the entire programme should be designed and implemented to be suitable for the target audience.

McCarthy (2006) wrote an article based on the findings of information security threats and responses survey which had been commissioned by the Computing Technology Industry association. The findings indicated that approximately sixty percent of the information security breaches experienced by organisations were caused by human error. However, despite this ominously high human error figure, of the companies surveyed twenty-nine percent only had required their IT staff to undergo security training while thirty-six percent only had offered their users information security training. McCarthy indicated that these findings were not satisfactory and that an information security awareness and training programme should permeate throughout an organisation.

It was noted that the decision makers, such as organisational executives, were often the least knowledgeable about information security despite the fact that they made decisions about this issue. This article indicated that it was essential that organisations expand the target of their information security awareness training and awareness programmes to users within their employee base, but outside of the IT department. The article emphasised the importance of making the organisational stakeholders aware of the necessity for an information security programme and also of the return on investment to be gained from the implementation of an information security programme.

Papanikolaou, Karakoidas, Vlachos, Venieris, Ilioudis, and Zouganelis (2011) presented a course based on conventional, well-established, theoretical frameworks of information systems security as well as on the unconventional challenges used by hackers to train newcomers. The reason for this type of course design is that Papanikolaou et al. (2011) were of the opinion that information systems security experts should be able to handle new and unknown threats or situations. Thus, they maintained that it was essential to foster an "out-of-the-box" capability and mentality as part of the education about the necessary skills required if this were to happen. In order to understand the reasoning which culminated in the abovementioned approach, it is necessary to examine a summary of related work in information security teaching methodologies. Firstly, these authors reiterate the reasons why information systems security as well as information systems security experts in the various specialty streams are needed and, indeed, in high demand. This led to a discussion on how the experts may be created.
The high number of educational frameworks and architectures which have been proposed by various sources were highlighted with particular emphasis on what is required by international standards for training and awareness as well as what is also required in academic environments. Additions particularly relevant to this analysis included the possibility of integrating an education environment which was sufficiently flexible to suit the needs of learners and multiple target audiences with online education, attractive content as well as an attractive implementation environment and current content and material. The next topic addressed was laboratory set-ups with the advantages and disadvantages of each potential set-up being argued. Finally, the organisation of the training was addressed. A role-game approach was used in terms of which the students were confronted with a variety of exercises and topics. The final section of the paper addressed the framework of educational approach and architecture advocated by the researchers. Papanikolaou et al. (2011) then explain how the course was been enriched with the use of the Hackademic tool. This tool provides a virtual framework that allows students to perform hacking attacks and penetration testing in a deliberately vulnerable, but isolated, safe, and controlled environment. Currently, the tool presents ten scenarios, accompanied by related exercises. A full description of the way in which a scenario is dealt with is provided. An assessment and examination portion is included within the tool. Using both an experiment and a survey, Papanikolaou et al. (2011) found that the majority of the learners had found both the hackademic tool and educational approach adopted to have been beneficial to their education.

The content included within the course approach discussed included defensive tools and techniques, network management, password management, password cracking, reconnaissance techniques, logging and auditing, packet sniffers, intrusion detection, security analysis tools as well as several other topics. No guidelines were provided to explain how the content had been selected although the content included may, itself, serves as an example of the controls and skills which ought to be included as content in other courses for organisational users.

Pastor, Díaz, and Castro (2010) provided a description of state-of-the-art simulation systems designed for information security and information assurance education, training, and awareness. The paper was divided into two sections of which the first identified and studied many of the systems of interest. The simulators were classified according to their target audience, usability, learning curve required, and the level of detail, scalability, and the likelihood of their being used. The second section attempted to construct taxonomy from these simulators and is presented in a tabular format. Pastor et al. (2010) concluded the paper by stating that is would be desirable if future tools developed focused on enabling education in information assurance concepts, not for
university students only but also for anyone who is professionally interested in the subject matter. They also expressed their opinion that future tools should be easy to use and individualised, thus enabling a sound understanding of the concepts by making provision for “experiments” to be conducted in the students’ own environment. The target audience, content and presentation varied was different for each programme analysed.

Power and Forte (2006) described the launch of a "powerful, unique and comprehensive awareness and education programme for a global entity" (Entity X)'s employees in the form of a case study. The paper examined the design, development and implementation of an effective, economic information security programme which aimed to change and foster an information security culture within an organisational environment and with the users. The purpose was to show that information security was a priority. However, in order to deliver this message and to foster the requisite culture it was essential that the education approach adopted contain meaningful content and be delivered in a persuasive way. This would also succeed in escalating security awareness. In order to do this all the communications, intelligence as well as the awareness and education functions of the global security team were aggregated together and a campaign that was filled with real-world examples and real-time intelligence was devised.

This campaign was timely, engaging, and compelling to the workforce. The campaign comprised a three-phase approach. During the first phase efforts were made to engage all the staff members, economically and effectively, in the campaign. A five-point initiative was implemented to order to accomplish this. Firstly, an awareness and education taskforce with role players from various departments was formed. Secondly, a bi-monthly electronic newsletter was launched. Thirdly, a brief security PowerPoint presentation on the security responsibilities of Entity X’s workforce was included in the new two-day hiring orientation process. Fourthly, a global annual security day was instituted and, lastly, an e-learning module covering security fundamentals for the education of new staff and the remedial training of existing staff was devised. The second phase consisted of security training seminars for IT professionals, while the third phase consisted of delivering vital security-related intelligence and early warnings regarding threats to executives. In its entirety the entire educational programme in the case study was deemed a success. This success was indicated by supporting empirical evidence. Unfortunately, this success was brief although great strides had been made in successfully increasing the level of security awareness and improving the general security culture within Entity X. However, the executive leadership of the organisation realised that they preferred that both they themselves and their organisation’s workforce were less aware of all the information security threats and risks out there in their own environment.
Power and Forte (2006) recommended that the depth in which topics are covered in the various delivery mechanisms should depend on the target audience and on the requirements of the target audience. Examples of the content in the newsletters included password security, child safety online, laptop security, identity theft, e-mail security, home pc security, social engineering, virus/worm defences, internet usage, telecommunications security, back-up and recovery, economic espionage, physical security (office and home), business travel security and emergency preparedness (office and home). The e-learning module covered the following seven subject areas, namely, password management, user-oriented anti-virus measures, physical security (including laptop security), appropriate internet and email usage, software piracy, backing up files and counter-espionage.

Puhakainen (2006) explored the way in which information system users' compliance with information system security policies and instructions can be improved. Puhakainen (2006) commenced the research by author reviewing and evaluating fifty-nine of the current approaches to information security awareness. This analysis was performed in order to determine the state of the existing information system security awareness research and to ascertain whether or not there existed a comprehensive review of the literature on the existing information system (IS) security awareness approaches. The first finding of the analysis indicated that very few of the existing information security awareness studies had a theoretically grounded basis while the second finding indicated that many of the approaches had not provide empirical evidence about their practical effectiveness. Puhakainen (2006) was of the opinion that knowledge and application of design theories would help practitioners and scholars to understand why a particular information system security awareness approach could be expected to have the desired impact on the security behaviour of users. He attempted to introduce three design theories in order to help to improve the information systems security related behaviour of users by addressing the shortcomings detected in the earlier analysis. The collection of design theories proposed included a first design theory for IS security awareness training, a second design theory for IS security awareness campaigns and a third design theory for reward and punishment.

The intention of the first design theory was to improve user information system behaviour in respect of compliance with security policies and instructions via information systems security awareness training. The design theory is based on two kernel theories – the universal constructive instructional theory (UCIT) and the elaboration likelihood model. The universal constructive instructional theory “provides a framework for designing situational instructional theories to be used in creating customized instruction” (Puhakainen, 2006, p. 71) and consists of the following
three elements, namely, functions, basic components and situated possibilities of constraint systems (Puhakainen, 2006, p. 71). Each of these components is further subdivided into subcomponents which govern the objectives, content, content context, delivery and presentation of the training and course material.

In order to complete this approach, the UCIT framework is then combined with the second kernel theory mentioned, namely, the elaboration likelihood model. This model encourages an attitude change in users by means of the cognitive processing of persuasive arguments and cues (Puhakainen, 2006, p. 72). This theory was empirically tested by Puhakainen (2006). The test involved two interventions conducted in two different companies. The theory proved to be effective and useful in both the software company and the information logistics company where the interventions were performed. Thus, this proven effectiveness indicates that this proposed design theory for information systems security awareness training is relevant to the development of training in practice. The second design theory proposed by Puhakainen (2006) was the design theory for information systems security awareness campaigns. This theory was based on the convergence model of communication kernel theory. This theory explains that different individuals will perceive different realities and, therefore, when an individual receives or creates information he/she will interpret the information in a way which is unique to him/her. This interpretation will, in turn, be influenced by each individual’s own beliefs and understandings. It should, however, be understood that all these various individual perceptions and understandings may eventually, through information sharing, merge into a mutual understanding between numerous individuals. This theory provides the basis of Puhakainen (2006) second theory. This second theory proposed designing IS security awareness campaigns to allow information sharing between many of the segmented target audiences as this would lead to mutual understanding and agreement and, eventually, to collective action as regards undergoing information systems security awareness training. The effectiveness theory was established through argument and was not an empirically based research study.

The third and final theory proposed was the design theory for reward and punishment. This theory was based upon the kernel theory of operant conditioning, namely, the principles of reinforcement and operant conditioning. The theory implied that it was possible to change user behaviour by manipulating the environmental variables resulting from certain behaviour. In other words, what was being suggested was punishing violations of and rewarding compliance with IS security instructions.
This research identified the lack of a pedagogical basis in the development of information security awareness campaigns and training with this lack extending to the delivery and presentation of the material. This research recommended the amendment of this design flaw. Puhakainen (2006) empirical study of whether an information security awareness training approach based on a pedagogical design foundation indicated that such an approach could be effective. The delivery methods used in the first phase of the empirical research at the software company included instructor-led discussions and e-mailed lessons which were used as an educational activity. In the second company the delivery methods included an e-learning package, instructor-led discussions and exercises involving authentic customer documents. A major lesson learned from this paper is the need for pedagogical grounding for information security education and empirical proof of the campaigns effectiveness. Lessons for material delivery are also extracted. These lessons could be applied to and cybersecurity campaign.

Romney, Higby, Stevenson, and Blackham (2004) discussed an information security education model that had been developed at Brigham Young University. In terms of this model, learners are encouraged to learn information security through active participation in its development and implementation. In other words, students are encouraged to prepare lectures and laboratories collaboratively as part of the IT security teaching model. The approach used in this case study was based on the active-learning pedagogy. The material was typically presented as hands-on activities. Guidelines for the setting up of these lecture and labs were provided but they did not specify presentation practices. The hand-on lab activities may be perceived as an e-learning approach. The content covered in the course was extremely technical. There were, however, no separate guidelines suggesting what content should be included or selected for inclusion in the course although an examination of the examples provided suggests the possible course content.

Schultz (2004) presented the argument that the component of any information security solution that has the greatest return on investment (ROI) is information security awareness, training, and education. Ideally, employees who receive security training or who are attending security awareness sessions would be less susceptible to social engineering and other types of attacks than before they had received the training. In light of this Schultz (2004) argued for more information security training and awareness research so as to render these educational approaches even more effective and beneficial. According to Schultz (2004), it is essential that information security courses be relevant to the needs and preferences of the target audiences, aligned with the relevant organisational objectives as well as up to date with current technology and practices. However, no exact content selection guidelines or examples were provided. It is
strongly stated that “one-size-fits-all” educational approaches are not suitable, and neither are subliminal awareness techniques such as posters and slogans on stationary effective as the sole educational approach.

Sharma and Sefchek (2007) described a hands-on approach to teaching information security to students majoring in information systems. This approach forms part of the curricula at Ball State University, a tertiary education facility. The paper began by justifying the need for information security awareness in the modern-day information and cyber-activity-reliant climate. This justification is accompanied by an overview of a supporting literature survey. The structure and content of this research’s course was then described. The course creators had developed three different courses which could be taken as electives. The courses were split to ensure that content coverage was adequate and that there was a progression in the difficulty of each course with each component building on the other. The courses were structured in such a way that the first basic concepts of a particular aspect of information security were introduced and the students then had to carry out hands-on exercises to reinforce the concepts. The scope and design of the courses were then discussed as was the content covered in each component. This was followed by a description of the available laboratory infrastructure and the pedagogical principles underpinning the entire course. The unnamed pedagogy endeavoured to synchronise theoretical lessons and the associated laboratory work. Sharma and Sefchek (2007) asserted that this approach ensured that the level of excitement and motivation remained high throughout the course. It was found that the learners performed the best in the laboratory exercises where they had some prior knowledge of the subject material or where they were able to perform the tasks on their home PCs.

The first component of the course covered the fundamental concepts of information security and security architecture. The second component covered a further four modules. The first module reviewed operating system security concepts and techniques, the theories behind security and hardening a system. The second module comprised a comprehensive overview of the building and maintaining of firewalls within a business environment while the third module included computer forensics and investigation topics. The fourth module covered the fundamental concepts of data protection, disaster recovery and computer forensics. Finally, the third course component provided the student with an overview of the field of information security and information assurance. However, despite the fact that the course content is covered in vast detail, no reasoning for the specific content selection was provided. Nevertheless, Sharma and Sefchek (2007) indicate that creating the content and course exercises was difficult because, upon
entering the course, the students possessed different levels of prior knowledge and skills relating to the topics.

Shaw, Chen, Harris, and Huang (2009) reported on a laboratory experiment that investigated the impacts of hypermedia, multimedia and hypertext which were used in an attempt to impact upon and increase information security awareness within an online training environment for organisational users. The levels of security awareness which were required to be impacted upon included perception, comprehension, and projection. The paper begins by briefly defining information security awareness and describing the why there is a need for it. Particular emphasis was placed on the need for the ongoing fostering of a security awareness culture in organisations and this, in turn, according to Shaw et al. (2009) required a robust awareness programme. Several of the characteristics of such a robust awareness education programmes were then identified. Finally, the influence of media richness on the effectiveness of the online security awareness programmes was examined. The media examined included hypermedia, multimedia, and hypertext. The findings indicated that those learners who understood the perception and comprehension levels improved their understanding at the projection level, with the learners using the text material understanding it better at the perception level, while the learners with the multimedia material performed better at the comprehension and projection levels. It would, thus, appear that hypermedia may be considered to be more effective in security awareness education than multimedia while multimedia may be considered better than hypertext. It is, therefore, clear that a media-rich approach to information security awareness education constitutes an extremely effective presentation method.

Schweitzer, Gibson, and Collins (2009) described an active learning approach to undergraduate security education (future professionals). Their paper began by emphasising the need for effective information security awareness education programmes. The paper identified active learning techniques as an effective method of motivating and engaging students in the learning process. Schweitzer et al. (2009) then indicated that several institutions have developed active information assurance curricula at all levels. Schweitzer et al. (2009) themselves had successfully implemented an active learning curricula approach for information assurance and they conveyed the lessons they had learnt during the creation of this course and during the implementation process. They began by justifying their application of the active learning pedagogy to the creation of their course by listing the advantages of active learning pedagogy. These advantages included motivating and engaging the interest of the learners while encouraging learning and retention.
They then described their experiences in applying active learning techniques to computer security courses before going on to discuss their incorporation into the course of the more traditional active learning approaches, including role playing and classroom activities as well as their self-developed series of interactive classroom visualisations, a cyber-defence competition, an inter-school vulnerability assessment exercise and hands-on laboratory exercises. They had found the active learning inspired changes to the courses to be effective in motivating and engaging the students. However, there was no empirical evidence provided to demonstrate how truly effective the course material was. It is recommended that the requirements of the target audiences and also educational objectives of the curricula be used to guide the selection of course content. Some of the content covered in their course is mentioned but no guidelines are provided for selecting the exact content for inclusion into a similar course. Lessons about content selection and presentation of the content can be derived from this paper.

Siponen (2001) examined information security awareness as an issue which comprised several dimensions extending beyond the organisational context. Siponen argued that information security awareness and knowledge should constitute an integral part of the general knowledge of any individual who makes use of information in the modern-day information society. This is because information is embedded in all the everyday lives of all users, and information related threats or risks may affect anybody. In support of this assertion, Siponen outlined and explored certain key issues within the five dimensions of information security awareness. The aim of this exercise was to set up information security dimensions in terms of form and target groups by proposing a framework for awareness perspectives in order to raise certain issues and produce practical examples and, thereby, inspire future research. The first of these dimensions is organisational. In terms of this dimension several different target groups for security awareness may be identified at an organisational level. These target audiences include top management, IT/IS management, normal end-users and, possibly, third parties’ users. It was noted that it is advisable that the necessary information concerning information security issues be shared and that this information should be clarified to all the target groups. However, it was also argued that the information security needs of each target audience would be different.

The second dimension comprises the general public with the target audience in this dimension being subdivided into two groups, namely, IT/computer/IS professionals and other end-users. The main objective in respect of this dimension is to increase public awareness of relevant security issues. This is based on the argument that there are certain central information security issues of which every citizen using IT should be aware. The third dimension is socio-political with the target
audiences within this dimension including lawyers, public relations people, politicians, and the government. Information security awareness is an important concern within the socio-political dimension and also an important factor in terms of the overall well-being of society. The fourth dimension is the computer ethical dimension. The objective of this dimension is, firstly, to provide relevant information to ethics scholars and, secondly, to learn from and make use of their confusion. Finally, the fifth dimension is institutional education.

It was argued that the exact security awareness need of various target audience would differ and, therefore, the content selected for a course should be based on the needs of the specific target audience. Various types of suggested issues which should be covered in the various dimensions were mentioned and it is possible that content selection may be derived from these suggestions.

Stanley and Herold (2006) maintain that it is important that all employees, not only records and information management employees, be educated about information security. They indicate that this education and also constant communication would be necessary to teach employees how to protect the information involved in their daily activities. This is important as it may play a role in ensuring the continuance of the business. Their article then promoted SCORE’s five basic education principles and recommended their implementation as part of an information security programme within an organisation. These principles recommend explaining the reasons for the training in question and the users’ roles as regards the practices being taught, making the users aware of how they would benefit personally, engaging their interest to ensure that they learnt, emphasising the expected outcomes from the training and maintaining and improving the training effort. This article suggested in-person courses as the delivery method pertaining to the how of delivering material. As regards the presentation component of material the article recommended engaging the learners in the course through the use of video and other visual sources, making the session interactive and providing sufficient time for questions and discussions.

Stewart and Lacey (2012) examined the reasons why mainstream information security awareness techniques have failed to evolve at the same rate as automated technical security controls. This research was deemed necessary because, despite the fact that there have drastic and rapid improvements in technical controls, information systems have remained vulnerable because of human behaviour. Stewart and Lacey (2012) propose that one possible reason for this problem may be that the approach to information security awareness is unsuitable. The paper found that the development of information security awareness over the past few years has remained relatively stagnant while it has also lacked formal methodologies for identifying the communication requirements of target audiences. This, combined with the lack of knowledge which is
acknowledged as a major contributor to unsecure human behaviour, has led to ineffective and inefficient awareness and risk communications practices. These practices include information security awareness campaigns being executed as generalised broadcasts of facts with no consideration for the specific needs of target audiences and technical experts only communicating to the users involved the practices which they think the users should know.

The paper further identified that, in general, the way in which people’s information security awareness needs may have been influenced by culture or demographic or pre-existing beliefs about information security has not been taken into account. In an effort to find ways in which to improve information security awareness programmes the paper then examined bounded reality, mental models, and the extended parallel processing model. The paper then suggested improvements that could be made to awareness techniques and efforts. These improvements were based on both psychology and safety science and they included moving beyond merely providing the awareness facts and motivating people to comply with instructions. Technical experts were disapproved of for simply providing generic material. Instead Stewart and Lacey (2012) propose that the needs and requirements of audiences, which may have been shaped by their beliefs, etc., should be used to determine the requisite content of information security awareness courses. No specific audience, beyond unaware individuals involved with information systems, were identified as the target audience.

Tidwell (2010) proposed testing whether simulations and training about information security awareness within the context of a variety of security scenarios could influence the responses of the users of a virtual community to security policies, behaviours, and security breaches. Virtual Community of Practice (V-CoP) would be used as a test community for a new model for a comprehensive security programme that would incorporate initial training for those individuals who were members of a V-CoP as well as the ongoing monitoring and periodic testing of their information security knowledge. Part of this process would be to educate the members on the potential threats and damages that may arise from careless behaviour that compromised computer security and that may, in turn, lead to financial and other losses. V-Cop, has members who may be internal employees, external partners, the general public and even competitors. Exactly what material was to be included was not covered in detail. However, the major topics which would be covered included areas of security such as password creation, data sharing and security, computer viruses and how they may be responsible for massive data losses and untold hours spent by employees in working to repair the damages. The topics indicated would be covered via a wide variety of security scenarios and simulations while the material would be
delivered via a web interface. The presentation format of the material included scenarios and simulated events. Otherwise, no specific presentation details or guidelines were provided.

Valentine (2006) presented a multiphase methodology for the implementation of an organisation’s information security awareness programme. The purpose of this methodology was to create an efficient and cost-effective information awareness approach that did not include generic material. This paper began by listing real-world examples of certain security threats and problems. It then examined a few common problems within the “one-size-fits-all” information security awareness education programmes commonly used by organisations. It would appear that the main problem is that these courses are ubiquitously presented to every target audience with no consideration of whether or not the material is truly relevant to them. This approach, in turn, had problems such as cost-effectiveness, learnability and lack of any ability to update of material.

The paper then presented a three-phased methodology approach that could tailor information security awareness programmes to the specific needs of an organisation as well as to the needs of the intended target audience. This methodology consisted of the following three components, namely, assessment, identification, and education. The first step involved the "scoping" of what the organisation required to protect and how the educational material could assist in this. The second step comprised the identification of those individuals with access to specific data, their roles in the protection of this data and relevant security procedures. The last step involved the creation of the education material, based upon the requirements of the previous two steps. Valentine (2006) suggested that the educational material could be partially scenario-based. It was also suggested that the material should include incident response procedures.

Van Niekerk and Von Solms (2004b) examined whether the application of the outcomes-based education (OBE) pedagogy would be suitable for an information security education programme for end-users. The paper began by examining the need for both information security solutions and information security awareness. It then emphasised the roles that humans play in an information security solution and identified the need for a security culture. The paper then offered an argument for the implementation of user education to foster such a security culture. Elements of information security education were discussed. This education programme would target adult users with well-established values and beliefs which may, in turn, affect their opinions and perceptions.

A list of features that should typically constitute such an information security education programme was then provided. This list suggested that “everyone should be able to "pass" the course”; “employees must know why information security is important and why a specific policy
or control is in place”; “learning materials should be customized to the needs of individual learners”, “users should be responsible for their own learning” and “users should be held accountable for their studies”. A comparative analysis of these requisite educational features as opposed to the "features" of outcomes-based education was then conducted. It was found that some of the required elements were already present in outcome-based education. It was, thus, concluded that an existing pedagogy, namely, outcomes-based education, would be a sound pedagogical basis on which to design and develop information security education programmes. However, no empirical evidence was provided to support this theory.

Van Niekerk and Von Solms (2009) discussed the way in which the use of Bloom's taxonomy may improve organisational user educational programmes which did not previously have a pedagogical basis. The goal of the paper was to explain how to use the taxonomy properly to assist in ensuring that the level of educational content selected was suited to the intended target audience. Van Niekerk and Von Solms (2009) briefly explained that Bloom’s taxonomy of the cognitive domain, while the models detailing the levels of the taxonomy (Remember, Understand, Apply, Analyse, Evaluate, and Create) were presented and explained. It was explained how each level built upon its predecessor, adding new abilities and levels of comprehension to the learner’s repertoire. Each level stresses different skills while also placing major emphasis on the correct categorisation of knowledge dimensions. The knowledge dimensions presented and explained included factual knowledge, conceptual knowledge, procedural knowledge, and meta-cognitive knowledge. The authors explain that “activities within the six levels of the cognitive domain are usually combined with the one or more of the four types of knowledge in a collection of statements outlining the learning objectives of an educational program. Usually a learning objective statement will be used to create a set of learning activities”.

Van Niekerk and Von Solms (2009) then explain that taxonomy provides four “organising” questions which assist educators in understanding the learning objectives. These questions include “The Learning Question: What is the most important for learners to learn in the limited time available”; “The Instruction Question: How does one plan and deliver instruction that will result in high levels of learning for large numbers of learners”; “The Assessment Question: How does one select or design assessment instruments and procedures to provide accurate information about how well students are learning” and “The Alignment Question: How does one ensure that objectives, instruction, and assessment are consistent with each other”. Van Niekerk and Von Solms (2009) then make use of an information security education to describe the way in
which the taxonomy may be applied to both content selection and activity creation for information security education.

Von Solms and Von Solms (2014) try to address the lack of a curricula or extramural for cybersafety education for school children. The paper presents an introductory, but usable, guide to empower primary school teachers, specifically in Africa, to impart the basic principles of cybersafety to their learners. A set of very usable, self-explanatory, publicly available online video cartoons were identified for use as resources by teachers in discussing and stimulate cybersafety principles to primary school learners. The videos alongside other resources were bundled together as a curriculum. This curriculum is incorporated into the campaign presented in this thesis’s active research process. Section 10.3.2.1.1 discusses the curriculum in detail.

Yeo, Rahim, and Ren (2008) proposed and evaluated the use of persuasive technology in information security awareness. Persuasive technology is a computing system, device or application intentionally designed to change a person’s attitudes or behaviour in a predetermined way. Within this study, the authors focus on the supposition that human attitudes indicate a user’s behavioural disposition, and that changing an attitude can result in the modification of behaviour. Based on the aforementioned supposition, the authors proposed the use of persuasive technology to help improve information security awareness of end-users. Persuasive technology makes use of a number of strategies to influence and persuade users. It is an interactive process, and it alters and adjusts the pattern of interaction based on the characteristics or actions of the persuaded party (the user’s input and context). Strategies include simplifying behaviour, guiding behaviour, customizing the behaviour to the user, intervening when necessary, self-monitoring, surveillance, and conditioning. The researchers designed a web-based program based on the principles of persuasive technology. The program aimed to change user attitudes towards password management, e-mail management and virus protection. The program made use of the following persuasive technology strategies: tunnelling (guided persuasion within a process or experience) and influencing through language. The web-program involved a sequential navigation through information security concepts. Each concept was displayed separately. Navigation between the concepts was determined by the users answering a multiple-choice question on each page. If the user answered correctly they were praised, if they answered incorrectly they were informed of the correct practice and they were taken onto related concepts or question in order to re-enforce what was learnt. To evaluate the effectiveness of persuasive, web-based program as part of an information security awareness, he researchers developed an instrument based on the Theory of Planned Behaviour (TPB). The program was tested by means of a pilot study involving 30 users.
This pilot study involved the students attending presentation of the web-based program. The users were required to complete the evaluation instrument before and after the presentation. Analysis of the data gathered, showed that web-based program had successfully increased and improved the attitude of the user is involved towards secure behaviours in the three topics covered by the presentation i.e. e-mail management, password management and virus protection. This research demonstrated the importance of customization, persuasion, feedback, and re-enforcement.

This section has provided an overview of sixty-five literature sources.

3.4 Overview of literature findings

A total of sixty-five sources were included in the literature review. The reviewed sources included international and national standards, national imperatives, curriculum guidelines and published peer-reviewed academic research. The literature was analysed from the perspective of the three broad thematic questions. A summative view of the results and the analysis of the literature review is presented in Table 3.1 and Table 3.2.: The three broad thematic questions, and their mappings to Table 3.1’s and Table 3.2’s columns are as follows:

1. Who comprises the target audience of the educational effort?
   This question examines who was the educational effort’s target audience. The question also examines whether the children are educated. Answers which relate to this thematic question are displayed within the tabulated analysis results, in column 1, 2 and 3. Column 1 represents Organisational users. Column 2 Represents Everybody or all users. Column 3 represents children.

2. What were they educated about?
   The issue of interest is whether the awareness, training, or educational effort taught lessons or topics, which are relevant to information-security campaigns, or cybersecurity and cybersafety campaigns. The question “Did it provide guidelines about what controls and content should be included?” was asked under this thematic question. The affirmative answers are represented in Column 4.

3. How were they educated?
   The question examines what specific approaches were used to teach the learners about information security, or cybersecurity and cybersafety. This examination included considering specific underlying components, issues or processes of the educational effort
highlighted in the study, as being important, e.g., pedagogical design, delivery or presentation, recommendations, and methods, etc. Four questions from the analysis relate to this thematic question and are displayed in Table 3.1 and Table 3.2. Column 5 represents the answers to the question “Are guidelines provided for the presentation of the course material?”. Column 6 represents the answers to the question “Are guidelines provided for the delivery of course material?”, The answers to the question “Were technology-based channels used or suggested for the delivery or presentation of the material?” is displayed in Column 7. Finally, the answers in Column 8 answer the question “Was a specific pedagogical basis used for the design of the course?”.

Table 3.1: Summary of the results for the literature review’s broad thematic questions

<table>
<thead>
<tr>
<th>Standards</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC27002 (2013)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO/IEC27032 (2012)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIST800-12 (2004)</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIST800-16 (1998)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIST800-50 (2003)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>National Imperatives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The UK Cyber Security Strategy (2011)</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The National Strategy to Secure Cyberspace (2003)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Curriculum Guidelines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACM IEEE Curriculum Guidelines for Undergraduate Degree Programs in Information Technology (2008)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Academic Research</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Albrechtsen (2007)</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Albrechtsen and Hovden (2009)</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Albrechtsen and Hovden (2010)</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alnatheer and Nelson (2009)</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Atkinson, Furnell, and Phippen (2009)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page.
<table>
<thead>
<tr>
<th>Reference</th>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
<th>Column 4</th>
<th>Column 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aytes and Connolly (2003)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Bishop (2000)</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bryce and Klang (2009)</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chunying (2010)</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cone, Irvine, Thompson, and Nguyen (2007)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conklin (2006)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>De Lange and Von Solms (2012)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Da Veiga (2015)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Davidson, N., &amp; Silence, E. (2010)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desman (2003)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dodge, Carver, and Ferguson (2007)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Du, Shang, and Xu (2006)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Eminağaoğlu, M., Uçar, E. &amp; Eren, Ş. (2009)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Endicott-Popovsky, Orton, Bailey, &amp; Frincke (2005)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S. Furnell (2008)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Furnell, Gennatou, &amp; Dowland (2002)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Futcher, Schroder, &amp; Von Solms (2010)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Goucher (2008)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Goucher (2009)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>J. Grimson et al. (2000)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Hagen &amp; Albrechtsen (2009)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Hagen, Albrechtsen, &amp; Johnsen (2011)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Hentea (2005)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hentea, Dhillon, &amp; Dhillon (2006)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Hu &amp; Meinel (2004)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Johnson (2006)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Katsikas (2000)</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kritzinger and Smith (2008)</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Continued on next page.
### Table 3.1: Continued from previous page

<table>
<thead>
<tr>
<th>Source</th>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
<th>Column 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kritzinger &amp; Von Solms (2010)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Kritzinger (2015)</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Kruger &amp; Kearney (2008)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Näf &amp; Basin (2008)</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>May (2008)</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>McCarthy (2006)</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Papanikolaou, Karakoidas, Vlachos, Venieris, Ilioudis, &amp; Zouganelis (2011)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Pastor, Díaz, and Castro (2010)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power and Forte (2006)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Puhakainen (2006)</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Romney, Higby, Stevenson, &amp; Blackham (2004)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Schultz (2004)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharma &amp; Sefchek (2007)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shaw, Chen, Harris, and Huang (2009)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Schweitzer, Gibson &amp; Collins (2009)</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Siponen (2001)</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Stanley &amp; Herold (2006)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Stewart &amp; Lacey (2012)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tidwell (2010)</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Valentine (2006)</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Van Niekerk and Von Solms (2004)</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Van Niekerk and Von Solms (2009)</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Von Solms and Von Solms (2014)</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Yeo, Rahim, &amp; Ren (2008)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
Table 3.2 Analysis of the results for the literature review’s broad thematic questions

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total of all 65 literature sources reviewed</td>
<td>40</td>
<td>17</td>
<td>5</td>
<td>26</td>
<td>21</td>
<td>27</td>
<td>33</td>
<td>5</td>
</tr>
<tr>
<td>Total percentage of all 65 literature sources reviewed</td>
<td>62%</td>
<td>26%</td>
<td>8%</td>
<td>40%</td>
<td>32%</td>
<td>42%</td>
<td>51%</td>
<td>8%</td>
</tr>
</tbody>
</table>

The aim of the literature review is to examine the current cybersecurity-educational approaches and identify those factors attributed as having contributed to their success.

The first thematic consideration for the review was: Who does the educational effort targeted, as an audience? The majority of the literature sources dealt with organisational users (62%). A limited amount of literature acknowledges that everybody within society needs cybersafety or cyber-security knowledge and behaviour (26%). Less than 8% of the literature sources explicitly dealt with making recommendations or implementing interventions for children. This demonstrates the need for cybersecurity and cybersafety educational efforts, which target school children.

The second thematic consideration was: What were the target audiences being educated about? Most of the literature sources did not explicitly explain or make recommendations for the content covered or planned for inclusion in the discussed education effort. However, based on reports, 40% of the literature did name broad topics within which the content could be included. The majority of these sources, however, were intended for organisational target audiences. Of the 5 literature sources acknowledging children as a target audience, only 2 sources provided some recommendations of potential content. The main recommendation was to take into consideration the particular audience’s needs and context.

The third thematic consideration was: How were the target audiences educated. The specific underlying components, issues or processes of each educational effort were highlighted in the individual paper reviews. In terms, of the broad lessons learned:

- 32% of the sources provided guidance through discussion, or by an example for the presentation of the course material;
- 42% of the sources provided guidance through discussion, or by way of example for the delivery of the course material;
• 51% of the sources recommended or used a technology base for the delivery, or the presentation of the material; and finally,
• 8% of the sources explicitly reported designing their educational effort to be pedagogically grounded; but none of these sources specifically targeted children.

None of the sources were widely recognised as educational guidance for cybersecurity. Overall, the analyses show that there is a definite need for guidelines to develop cybersecurity and cybersafety educational efforts that target school children.

3.5 Conclusion

This chapter has provided a detailed literature review of the current approaches to information security, cybersecurity and cybersafety education. An extensive overview of past and current approaches was provided. The purpose of the chapter was to present an overview of the existing information security and cybersecurity educational efforts; and to extract lessons from the literature reports relating to the theoretical and practical issues (factors) within the creation, implementation, and management of a cybersecurity educational effort. Individual factors were described within each review. In Chapter 6 to Chapter 11, when the literature informed interventions, the narrative references the relevant works. Finally, this chapter has shown that there is a definite lack of educational efforts targeting children. Additionally, there is a definite lack of guidance for cybersecurity campaigns that target children. Thus, the chapter has further demonstrated the relevance of the thesis’ primary objective to "Produce actionable knowledge, which offers guidance for designing and implementing educational campaigns that educate school learners about cybersecurity and cybersafety."
4 Methodology and Research Process

“Our goals can only be reached through a vehicle of a plan, in which we must fervently believe, and upon which we must vigorously act. There is no other route to success.”

~ Pablo Picasso
This chapter provides an overview of the research process followed during this study. Firstly, it outlines the philosophical considerations of the overall study. Then it discusses the subsequent choices of research paradigm and methodologies.

4.1 Introduction

Research is something that people undertake in order to find out things in a systematic way, thereby increasing their knowledge (Bassey, 1990; Ernest, 1994; Saunders et al., 2009). It is a purposeful process that involves the systematic collection and interpretation of data in order to derive an answer (Cohen, Manion, & Morrison, 2007; Olivier, 2009). It involves philosophical assumptions, research strategies, and methodological choices.

Regardless of exact procedure all research will include linked research stages that involve:

- formulating and clarifying of a topic (identifying the research problem),
- reviewing of relevant literature,
- formulation of the research design,
- negotiation and addressing of ethical issues,
- collection of data,
- analysis of data, and
- reporting (writing up) data and the communicating of the research findings and recommendations (Creswell, 2007; Saunders et al., 2009).

Within the research conducted for this thesis, these stages have all been iteratively revisited and thus the descriptive reports upon them will appear in multiple places. To ensure readability of this reporting extensive cross-referencing has been used.

An initial literature review was conducted to identify a problem, which was a ‘gap’ in the current research field. The identification of the gap led to the formulation of a problem statement, research questions, and objectives. This part of the research process formed stage 1 and was presented in Chapter 1. The remaining chapters of this treatise and the appendices present the other stages of the research. In order to ensure that the research presented in future chapters will be interpreted in a manner that matches the researcher’s viewpoint this chapter will outline the researchers’ choice of research philosophy and the implemented research design.
Chapter 4 Methodology and Research Process

The aim of this chapter is to provide details about the overall research process followed by:

- Providing insight into the philosophical assumptions of the author during this study; and
- Providing a brief discussion of methodological considerations and choices made for this study.

Within the next section the research design and choices of this study are discussed using “the research onion” as described by Saunders, Lewis and Thornhill (Saunders et al., 2009).

4.2 Research Design

In order to address a problem or answer a question, researchers follow an inquiry process. The process followed takes into consideration: the research philosophy they follow; and the aim, context and boundaries of the study, to ensure that the researchers arrive at a conclusion at the end of the study and that the result of study can be communicated (De Vaus, 2001). The purpose of communicating this research design is to provide the research findings with a level of credibility (Saunders et al., 2009). A well-designed research process helps to ensure a study’s success.

Several research design choices must be made in order to design an effective research strategy. These choices include decisions on which specific data collection techniques and procedures are necessary to complete the core research goal, as well as the philosophical assumptions that the researcher adopts. Some of these decisions must be made at the start of a study; others are made in later research stages as issues relating to them arise. Creswell (2003) recommends the adoption of a general framework to provide guidance about all facets of a study, from assessing the general philosophical ideas behind the inquiry to the detailed data collection and analysis procedures.

Saunders et al. (2009) developed an illustrated summary of effective progression through the research choices necessary to formulate an effective research methodology, using the metaphor of an onion. Figure 4.1 presents an illustration of the research onion.

The research onion has several layers, each representing a specific type of choice. To use the research onion, the researcher begins their process by making the choices from the outermost layers and then working their way towards the central or innermost layers. This is necessary as
the choices made in the outermost layers impact the choices made in inner layers. The layers of the onion, from the outermost to innermost layer, deal with the following issues:

- the research philosophy adopted by the study;
- the research approach taken during the study;
- the research strategy implemented
- the methodological choices made;
- the time-horizon of the study; and
- the techniques and procedures used for data collection and data analysis (Saunders et al., 2009).

The forthcoming sections of this chapter will briefly describe each of the choices made within each of the research onion’s layers for this particular study.

4.2.1 Research Philosophy

Research philosophy forms the outermost layer and the first research choice in the design of this study’s methodology. Research philosophy relates to a researcher’s world-view and tacit
assumptions about the nature of what constitutes acceptable knowledge and a knowledge development process (Guba, 1990). A philosophical paradigm defines these assumptions as an encompassed basic belief system or world view that guides an investigation (Saunders et al., 2009). It implies a pattern, structure and framework or system of scientific and academic ideas, values, and assumptions. Regardless of whether a philosophy is formally acknowledged, all research is conducted on the basis of some fundamental philosophical assumptions (Creswell, 2007, pp.15).

A number of research paradigms exist. Each paradigm has a particular view about the relationship between the nature of knowledge and the process by which that knowledge is developed (Saunders et al., 2009). This view will therefore guide a researcher in how they understand a research question, and it will impact the process through which they research it and its answer. Therefore, a research philosophy will have a significant impact on how research is conducted, and how its results will be interpreted and understood.

Core research choices which will be affected by philosophy will include the fundamental ontology and epistemology of the study (Saunders et al., 2009). These choices in turn would also affect several other components of the research process, including the choice of research strategy and research methods to be used. Therefore, understanding and choosing a research philosophy is a key step in planning and carrying out research. This section will outline the base assumptions of the various research paradigms. It shall conclude with a summary of the research paradigm selected for this thesis.

The choice of a paradigm is based upon the practical considerations of the study, and the suitability characteristics of a paradigm for the study. A paradigm is characterized by the following metaphysical characteristics: ontology (the assumptions relating to reality), epistemology (assumptions relating to how knowledge is generated), axiology (the roles of values in the research) and methodology (the sways of knowing reality) (Cohen et al., 2007; Crotty, 1998; Guba, 1990; Hanson, Creswell, Plano Clark, Petska, & Creswell, 2005). Together these characteristics influence one another and form the paradigm. The way these characteristics influence one another will now be briefly discussed.

The ontological characteristic of a paradigm deals with what the researcher or study views as reality. It deals with the nature of being and the view of what “exists” (Crotty, 1998). The choice of ontology affects the choice of epistemology. The epistemological characteristics of the
paradigm deals with how something is done from the researcher’s perspective. It examines the researchers perceived relationship with the knowledge which is being learned i.e. is the researcher’s perspective of the knowledge objective or subjective (Creswell, 2003; Ernest, 1994).

The ontological stance influences the epistemology. For example, a strict positivistic ontological view where the results (generated knowledge) would not be open to interpretation but rather be governed by strict guidelines of rules, the researcher would have an objective epistemology. In contrast, when various researchers may interpret generated knowledge, the research has a strong subjective epistemology. The choice of epistemology thus finally influences the choice of axiology and methodology. Axiology is the place of values in the research. Methodology in this context refers to the strategic approach to finding something out. It relates to the type of data sought and how to find it.

There are large varieties of paradigms based on the various combinations of the stances that can be taken within these characteristics. On one side of the spectrum, a researcher, whose philosophy tends to make use of quantitative data, believes reality is a concrete structure governed by laws and believes knowledge can be evaluated objectively tend to favour a positivistic paradigm. In contrast, a researcher on the other side of the spectrum could favour interpretivist or phenomenological views. An interpretivist will favour philosophy which involves value-bound research with a focus on gathering insights into subjective meanings of qualitative data gathered from in-depth investigations with small samples. Between the aforementioned paradigms there exists the pragmatic paradigm.

Pragmatism does not expect to find unvarying causal links or truths but aims to interrogate a particular question, theory, or phenomenon with the most appropriate research method (Feilzer, 2010). Pragmatic researchers believe that the importance of research is in the findings’ practical consequences (Cherryholmes, 1992; Saunders et al., 2009). Therefore, their focus is on the research problem and questions rather than on research methods. Within their research, pragmatists assume “that beliefs about reality, causality, and objectivity are context dependent and change, not always in predictable ways” (Cherryholmes, 1994). Therefore they are not committed to any one philosophical view of the world (reality) and they prefer to select research methods, techniques and procedures based on their needs and/or purposes (Cherryholmes, 1992, 1994; Feilzer, 2010). Consequently, pragmatists will also make use of quantitative and qualitative data as necessary.
The research conducted in this thesis follows a **pragmatic research philosophy**. In essence, pragmatism is a philosophy which prefers action to philosophizing (in a sense it is an anti-philosophy) (R. B. Johnson & Onwuegbuzie, 2004).

Section 1.6 outlined the research question of this thesis. Section 1.7 introduced the related primary objective of the thesis which is to “**Produce actionable knowledge, which offers guidance for designing and implementing education campaigns that educate school learners about cybersecurity and cybersafety.**”

The research question and its related objective deals with a problem at a societal level, even though it targets children. Within such a large scope, several philosophies and paradigms could be adopted by this study. A number of variables, theories, and viewpoints from within the philosophical continuum could be applicable to different issues and cycles of the research process. Therefore, the researcher could not subscribe to a single strict viewpoint e.g. strict positivism or strict interpretivism.

It is the belief of the researcher that all the research’s strategies, methodological choices, techniques, and procedures need to be selected based on their applicability or suitability for use on specific problem-solving task or activity being carried out. This belief combined, with the challenges of addressing a research question with a societal nature, resulted in this researcher searching for a wide-ranging philosophy, which focused on the outcomes of the research rather than the rigor or the research methods used. As a result, pragmatism was the philosophy of choice for this thesis.

### 4.2.2 Research Approach and Data choice

The research approach adopted relates to the form of logical reason used within the study. The reasoning approach taken while conducting research can be inductive or deductive in nature (Bryman, 2012; Saunders et al., 2009).

According to Saunders et al. (2009) a deductive research approach involves the testing of a theoretical proposition using a research strategy specifically designed for the purpose of its testing. Thus, the typical aim of this type of research is to test a known theory in order to gain evidence to support or refute the stated hypothesis. The direction of the research moves from the general to the specific.
An inductive research approach is the opposite of the deductive approach. An inductive research approach involves developing a theory as a result of the observation of empirical data (Bryman, 2012; Saunders et al., 2009). The aim of this type of research is to generate a theory of broad generalizations from specific observations. This the direction of the research moves from the specific to the general.

Several issues are addressed in this thesis in order to address the research questions. The nature of this thesis’s research approach to reasoning while addressing these issues is both inductive and deductive. Most of the reasoning conducted was **inductive** in nature. However, when applicable for certain issues, and when sufficient quantitative data was available, **deductive** reasoning was also used.

### 4.2.3 Research Strategy

The research strategy layer of the onion addresses the “plan” for how the researcher will proceed in answering or addressing the research question/s (Saunders et al., 2009). Researchers can use one or more strategies within their research design as the plan how to go about answering a research questions or addressing a research question (Creswell, 2003). Examples of approaches include experimental research, interviews, case studies, systematic literature reviews, surveys, ethnography, grounded theory, case studies, and action research.

This study conducted an annual cybersecurity education campaign targeting schoolchildren. Through the years, various theories, and interventions, were tested during this campaign. Data was gathered and analysed from each year’s campaign. The gathered data predominantly focuses on a single school that participated in the campaign every year; however, data from other schools was also examined when applicable to the issue of interest. Improvements are made to the campaign based on the results of the various interventions.

Two research strategies were of interest to this research: case studies and action research. These strategies will be briefly discussed:
1. Case Study

A case study is a strategy of inquiry that explores/investigates a particular contemporary phenomenon within its real-life context, using multiple sources of evidence (Creswell, 2009; Yin, 2009). Yin states that the research process a case study follows is a linear but iterative process. Within the process Yin describes six iterative stages namely the: “Plan”, “Design”, “Prepare”, “Collect”, “Analyse” and “Share” stages (Yin, 2009) The entire process is displayed in Figure 4.2.

Yin describes the purpose of the stages in the case study process as:

- **a. Plan** – The identification of research questions or other rationale for carrying out the case study;
- **b. Design** – The design of the research process for the study in order to demonstrate rigor;
- **c. Prepare** – a preparatory interval where the researcher must hone skills as a case study investigator; train for specific case study; develop case study protocol; conduct pilot case and gain approval for human subject’s protection;
- **d. Collect** – the implementation of the designed case study protocol, consults multiple sources of evidence, creates a database, and maintains a chain of evidence;
- **e. Analyse** – the analysis of the data (the displaying of the data and the interpretations of the data);
- **f. Share** – the sharing of the conclusions (Yin, 2009). Case studies are best suited for problems, which require a research strategy which focuses on developing an in-depth
understanding and analysis of the characteristics of a real-life instance of a case or multiple cases (Creswell, 2009). It is an appropriate research strategy in a research process where:

- The research addresses “how” or “why” questions;
- The investigator has little control over events;
- The focus is a contemporary phenomenon within a real-life context (Yin, 2009).

2. Action Research

Action research is a strategy which was initially proposed by Kurt Lewin, as a form of research which would lead to social action (Lewin, 1946). As proposed by Lewin, action research is a cyclical, iterative approach to research that involves iteratively solving a problem within a community of practice. Lewin’s proposed process involves the following steps:

1. identifying a general or initial idea;
2. fact finding about the idea,
3. planning the research process for addressing the idea or issue,
4. taking the necessary action step,
5. evaluate the research results, and then
6. amending the plan (Lewin, 1946; McNiff, 2002).

These basic action research process’s steps are illustrated in Figure 4.3. The process continues until the research study is concluded or the stopping of the process can be justified.

Figure 4.3: Action Research Process (Adapted from Lewin (1946) and Coghlan & Brannick (2010))
Over time, action research has become a research practice, with many schools, theories, and practices and is used in many subject fields (Baskerville & Myers, 2004). However, it does have some key features or characteristics, which are as follows:

- It encompasses a broad spectrum of research values and approaches,
- Action research is open-ended and does not begin with a fixed hypothesis. It involves identifying a problematic issue or idea, imagining a possible solution, trying it out, evaluating its results or effect, and changing practice based on the findings of the evaluation (McNiff, 2002). This process can be repeated as necessary. While imagining possible solutions underlying theories may be considered, adjusted to facilitate an outcome and then used to evaluate the action taken (Baskerville & Myers, 2004).
- It involves the management of a change and uses multiple research techniques aimed at enhancing change and generating data for knowledge production.
- It is “research in action rather than research about action” (Coghlan & Brannick, 2010). This type of research focuses on acquiring knowledge through action that is taken to improve a practice. It generates knowledge about how and why the improvements (or lack of improvements occurred (McNiff, 2002).
- It involves close collaboration between practitioners and researchers (Coghlan & Brannick, 2010; Saunders et al., 2009). It also commits to mutual learning between problem owners and researchers.
- The research result of action research is the production of knowledge based on solving real-life problems. The output is ‘actionable knowledge’ that is useful to both the practitioner and academic communities (Coghlan, 2007).

This form of research is suitable for exploratory studies require a strategy that meets the above characteristics.

An argument could be made to say that this research made use of a case study strategy. A dataset from a particular school was predominantly used from a specific campaign (context) to address a specific overall issue of fostering a culture amongst the children to make them cyber aware (phenomenon). This was to observe and analyse a particular phenomenon. However, the phenomenon being analysed was being influenced by the educational campaign that was being iteratively altered each year based on previous year’s results. The researcher was evaluating the results, amending the plan, and then taking action again. Therefore, this research made use of
an action research strategy, which incorporated case studies as a method as part of their data gathering.

The intent of the study was to produce knowledge for the guidance of future education campaigns, which aim to educate society about cybersecurity, based on the lessons learnt from attempting to solve the real-life problem in this studies context. The lessons learnt are supported within this strategy by evidential and narrative argumentations. Chapter 6 discusses further detail about the implementation of this study’s action research process.

### 4.2.4 Methodological Choice

This layer of the research onion calls for a methodological choice to be made. The research method is a strategy of enquiry, which moves from the underlying assumptions to research design, and data collection (Myers, 2013). It addresses the issue of whether the research study should make use of quantitative method/s and data, qualitative method/s and data or a mixture of both (Saunders et al., 2009). The choices outlined in the research onion include the mono method, the mixed method, and the multi-method (Saunders et al., 2009).

The choice of research philosophy and approach selected in previous layers of the research onion strongly influences the methodological choice. The researcher selected pragmatism as her primary philosophy. Part of this viewpoint is that no single viewpoint could fully explore or explain a research problem/answer. Pragmatists may use a one or many of data collection techniques analysis procedures as required provided it is necessary to enable the collection of credible, reliable, and relevant data. Thus, the philosophy encouraged the collection use and analysis of qualitative and/or quantitative data when it was necessary to address the research problem being addressed (R. B. Johnson & Onwuegbuzie, 2004). The research approach was identified as being primarily inductive but deductive reasoning was also applied as necessary. An inductive approach is often characterized as placing emphasis on the collection of qualitative data while, a deductive approach emphasis the collection of quantitative data.

For this research, data was collected and analysed for multiple issues within different cycles of the entire research process. A flexible research structure was used within the in the action research cycles and thus both types of data had to be used an analysed as depending on the focus of the research at the time. Therefore, mixed methods are used for the study.
Mixed methods research is a methodological approach suitable for pragmatic research as it offers the ability to make use of quantitative methods to measure some aspects of the phenomenon in question and qualitative methods for others (Feilzer, 2010).

### 4.2.5 Time Horizon

The second last layer of the onion is the time horizon under which the research was undertaken. The time horizon is independent of the research strategy (Saunders et al., 2009). The time horizon of a study can be longitudinal or cross-sectional. Longitudinal research refers to a study which takes place over an extended period of time (Saunders et al., 2009). Comparatively, cross-sectional study research refers to a study of a phenomenon or set of phenomena, which occur at a particular point of time (Saunders et al., 2009).

The time horizon considerations for this study mostly relate to the studies conducted during the various action research cycles. This research aimed to discover the factors to be considered when attempting to educate a society about cybersecurity. The third secondary research objective involved using an action research process to investigate factors that contribute to educating broader society about cybersecurity. Meeting this objective involved a process of several intervention cycles on at multiple schools in a particular metropole. Some schools were involved in multiple iterations within the research process interventions, others were not. The action research process began with its pilot cycle in 2011, and (for the purposes of this thesis) it concluded in 2015.

The primary dataset examined in the research originated from a single school that had been involved in every cycle of the study excluding its 2011 pilot study. The time horizon of the action research process within this study is predominantly longitudinal, because the majority of the findings of each research cycle relate to data gathered over the four-year period, from 2012 to 2015.

However, within certain research cycles not all the inferences drawn from the data are attributable to the primary dataset. Within certain cycles of the action research process and depending on the issue addressed, secondary datasets from schools that were intermittently involved in various research cycles were also gathered. Within these cycles’ relevant data from both, the primary and secondary datasets were examined when available and appropriate. Therefore, in some cycles of the action research process, the study’s time horizon was cross-sectional for specific issues.
4.2.6 Techniques and Procedures

The selection of a technique or techniques to obtain data, and the design or selection of the procedures required to analyse the data, make up the final stage within the overall research design. The data collection and analysis are dependent on the methodological approach used (Bryman, 2012).

This research design includes the use of mixed methods. Various stages of the overall research process and within the action research process addressed multiple issues of interest. There are a number of research methods, techniques, and procedures used for specific elements of this study. The details of the techniques and procedure used are outlined in the specific chapters to which they apply.

4.2.7 Overview of Choices Made for this thesis

The research onion, as presented by (Saunders et al., 2009) and discussed in the previous sections serves as a form of an agenda for laying out the research process taken. Its purpose is to enable the author to provide an explanation for how the various decisions made at each "layer of the research onion" had implications for the decisions made within the layers. The previous sections discussed the decision made for the research conducted for this thesis. As a summary, this section provides an overview of the philosophical, strategic, and methodological choices made and discussed in this chapter. Table 4.1 presents the summary of the research design choices.

Table 4:1: Summary of Research Design Choices

<table>
<thead>
<tr>
<th>Layers of Research Design</th>
<th>Decisions and Choices of this thesis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Research Philosophy</strong></td>
<td>The research process conducted followed the philosophy of <strong>pragmatism</strong>. The researcher prescribed to neither a strictly positivistic nor an interpretive perspective.</td>
</tr>
<tr>
<td><strong>Research Approach</strong></td>
<td>The research conducted was both and <strong>inductive and deductive</strong>.</td>
</tr>
<tr>
<td><strong>Strategy</strong></td>
<td><strong>Action Research</strong> was selected as the primary research strategy. The theoretical guidelines</td>
</tr>
</tbody>
</table>
of an action research study are presented in Section 4.3. The strategy was supported by evidential and narrative argumentation.

<table>
<thead>
<tr>
<th>Methodological Choice</th>
<th>Mixed Methods were used. Both quantitative and qualitative data was gathered and analysed depending upon the issue being addressed at a particular stage of the research process.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Horizon</td>
<td>The majority of the research process has a longitudinal time horizon. However, within certain research cycles (for particular issues) used “snapshots” of data from multiple datasets and thus these cycles had a cross-sectional time horizon.</td>
</tr>
<tr>
<td>Techniques and Procedures</td>
<td>To be discussed in relevant chapters and sections. Each of the action research cycles considered different theories and possible roles they could play. Techniques and procedures were chosen (and will be focussed) during each cycle.</td>
</tr>
</tbody>
</table>

This study used publication of theories and related results at/in relevant, peer-reviewed, subject specific conferences/journals as a primary form of verification of results and findings.

### 4.3 Research Process

This thesis focuses on producing actionable knowledge, which offers guidance for educating broader society about cybersecurity. This section outlines the research process followed during the study while trying to achieve this objective. The section begins with an outline of the work which preceded this research for context purposes. The preceding research and feedback obtained during its research process led to the identification of the problem addressed in this thesis. Additionally, it forms part of research process for the subsequent study. A full outline of the research process followed to address the research objectives of this thesis is then provided.
The research conducted within this thesis was preceded by a Master’s degree in the field of information security education. The prior research examined the need for the use of pedagogical principles in the design and presentation of cybersecurity education. The intent was to improve the probability of a campaign successfully educating a diverse target audience. The study demonstrated how brain-compatible learning principles can be used in the presentation of cybersecurity educational courses and to improve a learner’s learning experience and results. It thus proved that adhering to pedagogical principles when creating a cybersecurity course’s materials could contribute to the instructive success of the course. This initial work led to the publication of Reid, Van Niekerk, & Von Solms (2011) at the ISSA 2011 conference and Reid & Van Niekerk (2012) at the ZAW3 2012 conference (Appendix B).

The lack of a pedagogical foundation in most existing information security campaigns was a fundamental theoretical deficiency in many campaigns (Puhakainen, 2006). The application of pedagogical principles to a campaign which had lacked basis showed a related improvement in the overall success of the educational campaign. This success in turn showed that addressing theoretical deficiencies in campaigns could have merit and potentially improve the campaign’s success. This led to the questions of “What other theoretical deficiencies exist within these campaigns?”

There are several issues surrounding the establishment, maintenance, and success of cybersecurity education campaigns, which can target broad audiences. Feedback stemming from the initial Master’s work, and extensive literature work examining information security and cybersecurity education campaigns has led the author to believe that other factors and processes within a campaign can be similarly improved if they are designed or conducted following a sound theoretical basis. Thus, the focus of this research was established.

The research in this thesis aims to identify factors that could contribute to the success of cybersecurity audiences (school learners). The author conducted an exploratory study into this area of interest, leading to the research questions and objectives for this study. The author began by defining the research area, parameters, and open-ended issue of interest for the study, this portion of the research process is presented in Chapter 1, Chapter 2, and Chapter 3. Included within these sections, are descriptions of the definitions and the differences between an information security solution and culture; and a cybersecurity solution and culture. Publications relating to this aspect of the research included the publication of Reid & Van Niekerk (2014a) and
Reid, Van Niekerk, & Renaud (2014) at the ISSA 2014 conference. The remainder of the study was conducted in direct correspondence to each of the thesis’s secondary objectives.

The first secondary objective addressed was to determine the factors for consideration in the design and implementation of information security and cybersecurity and cybersafety education campaigns. The author conducted an extensive qualitative content analysis on existing literature in the fields of cybersecurity and information security education in order to identify was factors other research had identified and/or verified as contributing to the success of their awareness, training, and education efforts. Chapter 3 presents this component of the research.

The second secondary objective addressed was the identify existing theories from the fields of education and communication studies that can play a role in the improvement of the design and implementation of cybersecurity and cybersafety education campaigns. Numerous theories can be adapted and applied. Chapter 5 identified and discussed brain-compatible pedagogy and active audience theory.

The third secondary objective addressed was the investigation of factors, which contribute to educating broader society about cybersecurity using an action research process. This stage incorporated the results of the author’s Master’s research as part of its iterations. To meet the objective, the author initially became involved with an effort to establish a cybersecurity education campaign. The identified campaign was the South African Cyber Security Academic Alliance (SACSAA) school campaign.

The author was involved with the Campaign’s implementation by Nelson Mandela Metropolitan University (NMMU) from its pilot study year until the present year. As part of the campaign, an associated poster contest was run simultaneously each year. The cybersecurity educational campaign was conducted on an annual basis. Each year the success of the campaign was measure in terms of the learners’ level of internalization and topic adoption displayed by the learners’ posters.

Based on the factors identified in the literature and content, and on the feedback obtained from, and lessons learned in each year’s campaigns, the campaign was altered in order to improve its effectiveness. Chapter 5 to 11 presents the action research component of the study. Chapter 5 presents the theoretical basis of some of the changes or issues of interest in the various action research cycles. Chapter 6 to Chapter 11 presents the implementation details, and analyses, and
lessons learned, and subsequent factors of consideration for other campaigns, from each research cycle.

The author used a continuous process of publication and presentation of theories and results at relevant, peer-reviewed, subject specific conferences and journals as a method of gaining feedback from peers in the research field. This feedback formed part of reflexive practice which was carried out throughout the action research process (Alvesson & Skoldberg, 2000). Feedback included peer-reviews, and discussion with as many experts (and teachers) as possible. Reflecting on the results and the feedback received, assisted the researcher in making adjustments to the campaign and selecting issues of interest in the succeeding action research cycles’ issues of interest.

Publications, which stem from this portion of the research (excluding the previously mentioned publications from the Masters Research period), include:

**A. Journal Publications (Appendix A)**

**B. Conference Proceedings (Appendix B)**
Chapter 4 Methodology and Research Process


Finally, the last secondary objective was addressed as all of the lessons learned were integrated into a collection of usable, actionable knowledge in the form of guidelines and recommendations of factors to consider while attempting to educate broader society about information security. Chapter 12 presents the consolidated actionable knowledge. Further publication of this research will be pursued.

4.4 Research Design Considerations

Section 4.2.6 established that the techniques and procedures used to gather and evaluate data will be presented within their relevant research cycles. Similarly, the decisions relating to the design of the research including the specific decisions regarding interventions, the design of instruments, etc. will be discussed where most appropriate in the action research chapters they relate to).

4.5 Conclusion

This chapter provided an overview of the research methodology that this thesis followed. Using the research onion as a “guiding checklist” it presented the choices made for the study’s research design. Then it provided a detailed explanation of the actual research process followed in order to comply with the methodology and to meet the thesis’s research objectives. The work in this thesis was conducted in accordance with a pragmatic philosophy, which uses inductive and deductive approaches as necessary within its action research strategy. This thesis used reflexive methods that were informed by a continuous process of publication of theories and results at
relevant, peer-reviewed, subject specific conferences and journals as a primary verification method.

The next chapter will provide a description of the theoretical bases which influenced some of the action research process’s interventions.
Chapter 5 Theoretical Basis Used in Action Research Interventions

“While it is wise to learn from experience, it is wiser to learn from the experiences of others.”

~ Rick Warren
Chapter 5 Theoretical Basis Used in Action Research Interventions

This chapter presents a review of the literature to establish different theoretical bases or considerations that influenced the interventions implemented in the action research cycles (Chapter 6 to Chapter 11).

5.1 Introduction

The aim of this chapter is to provide contextual descriptions of the theories used in the practical part of the thesis. This chapter provides a discussion of the literature related to the theories used to assist in understanding their relevance when they are applied in the research cycles that will subsequently be discussed.

The work in this study is to a large extent based on transformative culture change theory when applied to information security, as discussed in Chapter 2. However, this work examines the theory in the context of cybersecurity and cybersecurity culture. The specific focus within the broader cybersecurity culture change process is the use of education as a transformative driver. As cybersecurity and safety education campaigns have a diverse target audience, such campaigns need to be designed to be as effective as possible in educating the majority of this audience effectively.

Cybersecurity is a societal issue which exists in a social sphere. As society becomes increasingly information-centric, the establishment of a cybersecurity culture is not only a technological problem, but also a social issue. Because cultures exist among peers, communities of practice and broader communities, a cybersecurity culture should be a sub-culture of such broader cultures. Cybersecurity education is then a societal responsibility (R. Von Solms & Van Niekerk, 2013). Designing educational material according to a pedagogy that complements the fulfilling of this responsibility is a natural decision.

The interventions used during the research cycles were based on a variety of theories. The most important of these are brain-compatible pedagogical theory and active audience theory. These theories were used during both intervention design and the analyses of results. This chapter presents these two theories.

The Chapter 6 to Chapter 11 will discuss the implementation of a cybersecurity and safety education campaign. Although this campaign was targeted at school learners the lessons learnt from it will be abstracted to apply to broader campaigns, which target a large and diverse
Chapter 5 Theoretical Basis Used in Action Research Interventions

audience. The cybersecurity and safety education campaign to be implemented takes into consideration the lessons learnt from the literature and similar campaigns elsewhere.

A fundamental issue that is identified in the literature and which affects the effectiveness of such a campaign is what the pedagogical foundation of such an education effort should be.

“Pedagogy” is an all-encompassing term concerned with what a teacher does to influence learning in others. Puhakainen found that many information security education approaches fail to pay sufficient attention to pedagogical theory (Puhakainen, 2006, p. 56). Thus, the application of pedagogical theory to the design and implementation of a campaign could contribute to improving the effectiveness of the effort.

Brain-compatible education is “a pedagogical approach to education which caters to the brain’s best natural operational principles, with the goal of helping learners attain maximum attention, understanding, meaning and memory” (Jensen, 2008c). Everything that humans do requires the use of their brain (conscious and subconscious cognitive thought). By learning more about the brain and applying that knowledge, efforts can be made to adapt learning material and experiences to suit the brain’s natural cognitive processing functions.

“Brain-compatible” or “brain-based” education is a well-established, successful pedagogical approach which builds on the understanding of the brain’s natural cognitive processing functions (Caine, 2005; E. P. Jensen, 2008b). The pedagogy was selected for use in this study, due to its well-documented success, its suitability for diverse audiences and its acknowledgement that education and learning is both individualistic and social.

Brain-compatible pedagogy was identified as being necessary in the early cycles of the research process and thus several implementation decisions made throughout the action research cycles were made in line with its pedagogical principles. These are discussed in the next chapter. The reason for taking into consideration the recommendations of brain compatible education was to assist in communicating cybersecurity messages to learners effectively.

Active audience theory was the second theory incorporated into the research during the final iteration of the action research process. During the campaign and the research process, questions arose as to whether the target audience was interpreting the security and safety messages the way the campaign intended them to be understood. The answer to this question is an indication of whether the campaign was successfully contributing to its envisioned ideal of a shared
Chapter 5 Theoretical Basis Used in Action Research Interventions

cognitive cybersecurity and safety culture among its audience. To answer the question, the audience and their interpretations of the campaign messages had to be examined.

The intention of a cybersecurity education campaign is to communicate certain messages (knowledge) to an audience, thereby influencing the audience’s opinions and views. Mass media, particularly television, has a similar intention, communicating messages or text for educational, entertainment and a plethora of other reasons. It is well established in social science research that the mass media has the ability to influence many aspects of people’s political, social and cultural agendas (Hall, 1977; Maxwell, 2012).

Cultural and media social science studies have found that audiences may interpret media messages differently. One theory that is used to explain the media’s communication process and the differences in audiences’ interpretation is active audience theory. This is second theory which will be examined, with a focus on the encoding–decoding model.

The author believes that the encoding–decoding model could be used, or adapted for use, in determining how the audience of a cybersecurity awareness campaign interprets the campaign’s intended message. There are two reasons for this belief. Firstly, cybersecurity and safety awareness campaigns share a goal with media, that is, they aim to communicate a message and influence their audience. Secondly, awareness campaigns make use of mass media and other similar communication formats.

Determining the audience’s decoding position when interpreting the message could assist in detecting either deviations or uniformity between the audience’s interpretations of the meanings of the messages and the meaning of the campaign’s intended message.

This section contains a discussion of these theories based on the literature. Brain-compatible education is discussed in section 5.2 and active audience theory is discussed in section 5.3. The applications of the theories and their principles to the design and implantation of the cybersecurity and cybersafety education campaign, and its material, are addressed in Chapter 6 to Chapter 11.

5.2 Brain-compatible Education

A pedagogy is defined as a “method and practice of teaching, especially as an academic subject or theoretical concept” (Oxford, 2016). Brain-compatible education is a pedagogy which acknowledges the brain’s “rules” for learning and then organises teaching with those rules in mind
Chapter 5 Theoretical Basis Used in Action Research Interventions

(Caine & Caine, 1991, p. 4). This section will introduce the pedagogy and outline some of its principles.

In all teaching environments educators endeavour to ensure that the students learn what is being taught. To encourage students to learn successfully, common objectives for the educator during the teaching process include to ensure that students

- focus on what is being taught
- attach new concepts to known concepts in order to derive meaning
- actively engage in the education experience, and
- demonstrate that they have successfully learnt what was taught (Banikowski, 1999).

The proof that learning has occurred requires the learner to be able to recall and demonstrate what was learnt. The ability to remember, that is, memory, is thus a crucial tool in the learning process.

Memory focuses on learning, linking and remembering the various fragments of knowledge and skills that have been learnt by an individual (Banikowski, 1999). Unfortunately, memory may occasionally fail learners during their studies and they will have difficulty remembering what was taught (Banikowski, 1999, p. 15). In order to encourage the formation of well-formed, permanent, or enduring memories it is essential that anything that is taught is as memorable as possible for the learner. Therefore, the implementation of a suitable pedagogy for teaching the material would be extremely effective in helping to accomplish this. The pedagogy should be suitable for a large audience and make remembering the taught material as easy as possible.

Over the past three decades there have been many advances in human understanding of the brain. This understanding has arisen from the converged findings of several research fields, the most predominant being neuroscience and psychology. The development of technologies such as positron emission tomography (PET), scanning, and magnetic resonance imaging (MRI) have made it possible to study healthy human brains (McGeehan, 2001).

Neuroscientists and psychologists have collaborated and communicated on the findings of these brain studies and the existing understanding of the human mind. They have found that an individual’s experiences literally shape the brain for survival (McGeehan, 2001). The brain changes as it learns from experiences and some studies have examined the changes in the brain following specific educational interventions. This has led to the identification of brain-compatible education principles. Appendix C presents the way the brain changes when learning takes place.
In brief, the learning of new concepts helps the brain to grow by building new neural pathways, dendrites and connections (Lombardi, 2008). Much research has examined this occurrence in the brain during learning processes. Some neuroscience researchers have identified which areas of the brain are, and are not, active during a learning experience (Erlauer, 2003; Jensen, 2005; Wolfe, 2010). Their research findings on the brain, combined with psychological insights into topics such as learning and memory, have resulted in a better understanding of the brain during learning (Bruer, 2006; McGeehan, 2001). Subsequently, educators have sought to take advantage of this insight into the function of the learning brain to improve their teaching methods.

Some educators and researchers have been making efforts to apply knowledge about the brain to aid learning processes. This has gradually led to the identification of environmental factors and implementation guidelines which may either assist or detract from student learning. Over time many practices, processes and principles have been designed to take advantage of the natural cognitive abilities of the brain. The aim of their implementation is to stimulate those sections of the brain that are involved in the learning practices. Collectively, these techniques have resulted in the development of the pedagogy known as “brain-based” or “brain-compatible” education.

The term “brain-compatible education” was coined by Leslie Hart and refers to an educational approach designed to match “course settings and instruction to the nature of the brain, rather than trying to force (the brain) to comply with arrangements established with virtually no concern for what this organ is or how it works best” (L. A. Hart, 1999). Similarly, Jensen defined brain-compatible (brain-based) education as the “engagement of strategies based on principles derived from an understanding of the brain” and Caine and Caine (1991, p. 4) Stated that “brain-based learning involves acknowledging the brain’s rules for meaningful learning and organising teaching with those rules in mind”. For the purposes of this research, brain-compatible education may be defined as education based on the principles, methods and techniques which endeavour to teach subject matter in a manner and format which is naturally complementary to the physical and psychological processing functions of the brain.

Brain-based education uses effective teaching methods, techniques and approaches from all the education disciplines to ensure that the subject matter is as appealing and learnable as possible for the brains of the target students (Jensen, 2008a). To achieve this, brain-compatible educators design and orchestrate lifelike, enriching and appropriate experiences for learners (Caine & Caine, 1991). All students can benefit from instructional strategies that may assist them in processing information more effectively so as to ensure maximum understanding, retention and recall (Banikowski, 1999, p. 15).
Educators can use brain-compatible techniques and strategies to positively influence, support and advance cognitive growth (Caine & Caine, 1991; Erlauer, 2003; Jensen, 2005; Sprenger, 2002). Such techniques are primarily meant to have educational (cognitive) benefits; however, they are also acknowledged to have a positive influence on learners’ social and emotional states.

Some brain-compatible strategies may be employed in any classroom in order to provide opportunities for the brain to transfer information to the short-term memory and then, further, to store the learnt information securely in the long-term memory (Wolfe, 2010). This is often carried out successfully because, in the context of a classroom environment, brain-compatible education techniques are able to address multiple modes of learning, acknowledge outlets for the creative presentation of learning, and provide sufficient contrast to preclude boredom and to contribute to a motivating context (Jensen, 2005; Jones, 2003; Rogers & Renard, 1999; Wolfe, 2010). Overall, the techniques aim at attracting the learner’s attention and ensuring that the learner processes the education experience in a way that promotes the extraction of meaning from the material (Caine & Caine, 1991).

Brain-compatible education encompasses several simple and neurologically sound principles as a general theoretical foundation (Caine & Caine, 1991). The next section will outline some of the principles which were deemed most relevant to this work.

### 5.2.1 Brain-compatible Education Principles

The purpose of brain-compatible principles is to manipulate a learning environment directly so as to foster students’ cognitive growth and understanding (Lombardi, 2008). When applied to educational material the brain-compatible principles guide educators in the definition and selection of appropriate educational programmes, methodologies, and presentation techniques.

A great deal of literature focuses on explaining the underlying biology of learning (Appendix C), and deriving brain-compatible education principles from an understanding of the brain during the educational experience. However, in the case of this thesis, no new principles are identified and/or proven. The thesis simply applied the principles identified in the literature.

All of the principles of brain-compatible education aim to match both the educational environment and instruction to the nature of the human brain so as to promote optimum learning and retention. The literature shows that it is important that educators become familiar with and understand the
Chapter 5 Theoretical Basis Used in Action Research Interventions

general categories of brain-compatible education techniques as a means of enhancing student learning (Abiola & Dhindsa, 2012).

This thesis will apply a select number of brain-compatible principles to the cybersecurity education campaign presented in Chapter 6 to Chapter 11. There are a number of reasons why only a select number of principles will be applied. Firstly, there is no definitive or complete list of brain-compatible education principles or of their implications for educational experiences and environments. Thus, identifying and applying every principle is unlikely to be guaranteed. Secondly, not all of the existing brain-compatible principles can be applied in this research, as some are unsuitable for application to the campaign.

An example of an unsuitable brain-compatible education principle would be “learning engages the entire physiology” (Caine, 2005). The recommended method for complying with this principle is the incorporation of stress management, nutrition, exercise and other health considerations into the learning process (Caine & Caine, 1991; Jensen, 2008b). In the campaign in the current study, this would be beyond the researcher’s control as the campaign is predominantly implemented in schools which have limited contact with the researcher and the subject experts.

Eight brain-compatible principles that have been deemed most relevant for the purposes of this thesis are shown in Table 5.1.

Table 5:1 Brain-compatible principles

<table>
<thead>
<tr>
<th></th>
<th>A learning experience should be as multifaceted as possible, catering for as many learning styles as possible and providing as many opportunities for each learner to develop as possible.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Positive emotions should be used to aid recognition and recall.</td>
</tr>
<tr>
<td>3</td>
<td>Relate all new material back to old material and thereby build new knowledge on old knowledge.</td>
</tr>
<tr>
<td>4</td>
<td>The search for meaning is innate and occurs through patterning.</td>
</tr>
<tr>
<td>5</td>
<td>Every brain simultaneously perceives and creates parts and wholes during the learning process.</td>
</tr>
<tr>
<td>6</td>
<td>It is necessary to review material repeatedly to solidify recall and recognition.</td>
</tr>
<tr>
<td>7</td>
<td>Both a learner’s focused and peripheral attention should be involved in the learning process.</td>
</tr>
<tr>
<td>8</td>
<td>Allow learners to progress through the course at their own pace.</td>
</tr>
</tbody>
</table>
These principles were selected on the basis of how important the researcher judged them to be in relation to the campaign; how possible it was to control the application of the principle to the campaign; and how convenient or available the resources and skills needed to apply the principle were. Other principles may have been catered to by coincidence, not design. However, such principles were not deemed as having had their application controlled by the researcher.

The principles listed in Table 5.1 are not in any particular order of importance or relevancy. However, when forthcoming chapters refer to the principles they will reference the number of the principle as it is shown in this table. The forthcoming sections will now discuss the practical applications of each of the principles as recommended by theory and the literature.

**5.2.2 A learning experience should be as multifaceted as possible, catering for as many learning styles as possible and providing as many opportunities for each learner to develop as far as possible.**

“Getting information is essential for learning” (Zull, 2006). However, the quantity and quality of the information which is gathered may be improved if the learner is engaged in the experience, as active engagement during a learning experience enhances both memory and learning (Banikowski, 1999).

Contemporary information processing theory studies show that a learner’s primary contact with the information or knowledge they are expected to learn is through their sense receptors (Banikowski, 1999). Students listen to their teachers (ears), read texts (eyes) and write, model, and interact through gestures (hands). For a brief time, an individual’s sensory register temporarily holds all of these sensations. Visual information lasts less than one second, tactile information one to three seconds and auditory information up to four seconds (Banikowski, 1999). Therefore, if nothing is done to actively focus the attention held in the sensory register, it is soon lost.

Bloom (1987) found that engaging individuals actively in learning results in the learners retaining 10% of what they read, 20% of what they hear, 30% of what they see, 50% of what they see and hear, 70% of what they say and 90% of what they say and do. To assist in actively engaging learners, the first brain-compatible education principle states that *each learning experience should be as multifaceted as possible; catering for as many learning styles as possible and providing as many opportunities as possible for each learner to develop as far possible* (Caine & Caine, 1990; Jensen, 2008c; McGeehan, 2001).
Chapter 5 Theoretical Basis Used in Action Research Interventions

The objective of this principle is to enrich every learning experience and to engage and motivate every learner during the lesson and the associated activities. As a whole, this principle promotes both the development of educational material which caters for the many different learning styles and lesson planning which accommodates the individual needs of students (Caine, 2005; Erlauer, 2003; Sprenger, 2003).

A learning style is “an approach to learning which favours the brain’s best natural operational principles, with the goal of attaining maximum attention, understanding, meaning and memory” (Jensen, 1995, p. i). An effective educational solution would be the use of several combined teaching strategies that promote learning across all learning styles (Materna, 2007). Thus, it is essential that instructors be encouraged both to be aware of the various learning style differences and to incorporate in their lessons the use of a variety of teaching approaches designed to cater for all these learning styles (Caine & Caine, 1991; NIST 800-16, 1998).

“Promoting activities that activate seeing, hearing and feeling facilitates much more productive, efficient and long-lasting learning” (Materna, 2007). The main sensory-based learning styles favour auditory, visual, or tactile material. Sousa (1998) found that, in a typical class, 19% of the learners are auditory learners, 35% are kinaesthetic learners and 46% are visual learners. In view of the fact that these styles are particularly prominent they should all be catered for.

5.2.2.1 Auditory learning

Auditory data is the core of language, which has both cognitive and emotional content (Zull, 2006). Learners who favour an auditory learning style understand educational material better after listening to the material (NIST 800-16, 1998). These learners are often communicative individuals and need to feel included and involved in their lessons. Examples of ways for education efforts to cater for these learners include the following:

- The inclusion of the active presentation of concepts in lesson or guest presentation format.
- Supporting educational material which is narrated to provide audible explanations of concepts.
- Topic discussions and the sharing of media encourage learners to communicate and collaborate with each other.
- Evocation of emotion through sound effects in demonstrations, explanations, and resources, e.g. videos.
5.2.2.2 Visual learners

Visual learners tend to have stronger spatial awareness than other learners and, thus, they are often able to perceive and understand forms of information which are represented in a spatially explanatory way. These learners are more likely to read, understand and retain information which is presented in a readable format or a graphic format, for example a graph, chart or image (Caine & Caine, 1991; Erlauer, 2003; NIST 800-16, 1998). An educational effort could cater for the visual learners by including

- presentations in a brain-compatible format including graphics, charts, diagrams, and animations
- videos of class lectures and scenario enactments which would serve to create an “in-class” feel, thus enabling the learner to feel as if they are in an inclusive learning environment (NIST 800-16, 1998)
- process flowcharts and chains which may be used as reference guides to understand the flow between concepts and activities.

5.2.2.3 Kinaesthetic-tactile learners

Kinaesthetic-tactile learners prefer to learn by being directly involved in the learning process (NIST 800-16, 1998). This learning style, much like active learning, is an educational approach which delivers content to learners using hands-on activities (Conklin, 2006). The use of hands-on activities may assist with the thorough exploration of new concepts and may allow abstract concepts to become concrete for the learner (Caine, 2005; Erlauer, 2003; Jensen, 2005; Smilkstein, 2011; Wolfe, 2010). Applications of this principle in educational efforts could include the following:

- Interactive lesson activities which help to engage the learners in the learning experience (NIST 800-16, 1998).
- Task simulations to enhance the learning experience and also to provide a sense of realism to the concept that learners may relate to.
- Games which emphasise the concepts taught in the lessons and assist the learners in gradually developing an understanding of the concepts.

Although each of these learning styles should be included individually, they are, in fact, the most effective when used in a combined approach. The brains of nearly all students learn best through
multiprocessing (Taylor, 2007). The more parts of the brain involved in a learning activity, the more likely it is that a strong memory will result and that what was learnt will be retained (Jones, 2003, p. 103; Scoffham, 2004). Accordingly, the optimum approach for the engagement of learners could possibly be “orchestrated immersion” (Gülpınar, 2005). Orchestrated immersion is achieved by creating a complex experience which involves all the sensory channels. Overall, this principle promotes education methods which provide optimal opportunities for learning by giving learners rich, complex and realistic experiences (Caine & Caine, 1991; Gülpınar, 2005).

5.2.3 Positive emotions should be used to aid recognition and recall.

“Intellectual learning and emotional involvement are linked together in the fabric of the brain.” The brain does not naturally separate emotions from cognition on either an anatomical or a perceptual level (Caine & Caine, 1991; Damasio, 1994; Scoffham, 2004) and permanent learning almost always has an emotional component (Carter, 2000; Erlauer, 2003). "Emotions give us a more activated and chemically stimulated brain, which helps us recall things better" (Jensen, 1998). Thus, students are more likely to attend to and remember information that is meaningful to them and which contains an emotional "hook" (Banikowski, 1999). This approach is effective because emotions focus an individual’s attention which, in turn, drives their learning and memory systems (Scoffham, 2004). Therefore, to take advantage of this natural occurrence it is essential that learners engage emotionally as well as cognitively in learning activities (Scoffham, 2004).

“Complex learning is enhanced by challenge and inhibited by threat” (Lombardi, 2008). Stressful, threatening or fearful emotions which are elicited during a learning experience are more likely to create memories of the negative issues which occurred rather than the important academic concepts (Erlauer, 2003; L. A. Hart, 1999). Conversely, fostering positive emotions in learners while learning will create opportunities for memories to form, thus enhancing the remembering of the academic concepts taught (Erlauer, 2003). This leads to the fundamentally important second principle of brain-compatible education, namely, positive emotions should be used to aid recognition and recall because “emotion is the gatekeeper to learning” (McGeehan, 2001).

For students to place a priority on learning, they must feel safe from both real and perceived threats (Jensen, 1995, 2008b; Rogers & Renard, 1999). Therefore, the establishment of an environment of “relaxed alertness” is recommended. Educational efforts should thus aim to create an optimal emotional and social climate (challenging, but a non-threatening and confirmative
environment with complex social interactions) for all learning activities in order to encourage learning (Gülpinar, 2005). The implications of this for educational efforts include the following:

- Material could be presented in a manner which relates it to issues or circumstances to which learners are able to relate personally (Banikowski, 1999). This is as a result of the fact that “learning occurs only when what is being presented is meaningful enough to the student that he or she decides to actively engage in the learning experience” (Caine & Caine, 1991). Being meaningful to the learner often means that the activity satisfies specific human emotions.

- The previously mentioned interactive lesson exercises, task simulations and games may also serve to engage the learner’s emotions and create a positive feeling as the learner relaxes in an entertaining environment.

- Feedback should be provided for all activities and interactions so as to give encouragement, positive affirmation and possible advice that relates specifically to an individual’s results and progress.

- Classroom discussions, scenario descriptions and role-playing activities may be used as they all serve to increase attention through emotional stimulation as well as resulting in a stronger activation of the brain processes.

- Material may be related to the common personal experiences of the individuals concerned, while reflection, interpersonal discussions and comparisons of the life experiences and points of view of various people may be encouraged, as these activities help promote cognitive, affective, and spiritual growth.

- Humour that is relevant to the subject and the lecture may be used in moderation throughout the course and its individual lessons in order to gain attention, elicit emotion and ease tension. Humour can be effective because laughter increases the functioning of the entire brain, allowing the brain to increase its capacity, and this state enables the person to simultaneously perceive the abstract, subtle nuances of a problem and its more concrete logical aspects (Lopez & Alipoon, 2000; Taylor, 2007).

Caution is required when implementing this principle especially in cases where feedback is provided. The intention of feedback should not be perceived by the learners as threatening, hurtful, unnecessary or inappropriate criticism (S. Rogers & Renard, 1999).
5.2.4 Relate all new material back to old material and thereby build new knowledge on old knowledge.

The possession of prior knowledge or experience which relates to current learning enhances memory while, conversely, a lack of prior knowledge or experience on the current learning reduces memory (Banikowski, 1999). In other words, “what we already know determines, to a great extent, what we will pay attention to, perceive, learn, remember and forget” (Woolfolk, 1998, p. 247, as cited by Banikowski, 1999).

The third brain-compatible principle involves relating all new material back to previously mastered material, thereby building new knowledge on old knowledge. This principle promotes assimilation – the process whereby an individual incorporates new experiences into an existing behaviour pattern (NIST 800-16, 1998). Thus, this principle encourages experts, educators, and material developers to identify any problems that may hinder a student’s learning and rate of understanding, that is, that which may prevent learning as a result of either its complexity or a lack of previous experience with any similar subject. After having identified all the possible hindrances, educators and material developers, while taking into consideration their knowledge about the way in which the brain chunks and categorises information, can devise the material in a way which will help the learners to connect new information to prior knowledge (Erlauer, 2003; Jones, 2003; Wolfe, 2010).

It is essential that brain-compatible material and efforts emphasise relationships and topics for learners that have both direct and indirect links between curricular areas, and also explain how the content overlaps. Thus, this style of teaching and learning encourages opportunities for the inclusion of experiential and authentic learning opportunities through hands-on, interactive learning simulations, the inclusion of interesting, related video or media snippets to act as “guest speakers”, as well as real-world examples and simulations which may act as “field trips” to aid learner understanding (Caine, Caine, McClintic, & Klimek, 2005; Erlauer, 2003; Jones, 2003). In addition, if the new information and skills are associated with or related back to issues about which the learner cares, the opportunities for the learner to derive the kind of meaning that will become a long-term memory will also increase (Caine & Caine, 1991; McGeehan, 2001). This principle may have several implications for the education efforts:

- Examples of new knowledge could be associated with “common” and daily life experiences (Abiola & Dhindsa, 2012; Caine & Caine, 1991).
• Presentations may include enquiry questions. These enquiry questions engage the learners and help them to relate what is being learnt to their previous knowledge and, thus, they are able to derive an understanding of the material.

• Metaphors, analogies and imagery may be included (Banikowski, 1999).

• The previously mentioned slides, videos and task simulations can often be related to real-life problems. This may be extremely effective as situational training immerses an individual in a familiar environment and may improve the efficiency of his/her processing abilities (Chen et al., 2008).

• Activities and resources that demonstrate concepts may also be embedded in the lessons, for example the task simulations and videos.

• Topics being taught could be organised so that previously learnt information is used for the learning of new knowledge (Abiola & Dhindsa, 2012). The sequential grouping of content, lessons, presentations, and related activities could assist learners to cognitively recognise the relationships between what is being taught and the knowledge it is being related to.

The one potential disadvantage of this principle is that it is dependent on the previously learnt knowledge and behaviour of the learners. However, this may be countered by ensuring that the education experience creates the prior knowledge and experience (Banikowski, 1999). The vast potential for growth that this principle presents to any learning experience ultimately renders it a valuable principle for application to learning situations. It should also be noted that the principle is closely related to the principle relating to the “search for meaning”. Any search for meaning occurs through patterning, with patterning beginning with the brain searching for similar, prior knowledge and experiences (Lombardi, 2008).

5.2.5 The search for meaning is innate and occurs through patterning.

The brain wants to make sense of what it learns and it wants to know that learning has both purpose and value (Lombardi, 2008). When educators share with learners the rationale for what they are doing, the brain and the learner value such learning more deeply. The fourth brain-compatible principle states that the search for meaning is innate and occurs through patterning. This may be regarded as a principle for the following two reasons: Firstly, the search for meaning is survival-oriented and is basic to the human brain (Caine & Caine, 1990) and, secondly, the brain is likely to store most effectively what is meaningful to the learner from the learner's
perspective (McGeehan, 2001). Students learn more effectively when their interests and ideas are engaged and they perceive what is being taught as valuable (Caine et al., 2005, p. 67; Rogers & Renard, 1999).

The more the brain is able to make sense of what is being learnt, the more time there is available for higher-level thinking and thorough application of the lesson’s skills (Caine, 2005; Erlauer, 2003; Jensen, 2005; Sprenger, 2003; Wolfe, 2010). During the learning process, the brain attempts to distinguish and understand the patterns which appear in what is being learnt or experienced. Caine and Caine (1991) explain this as “patterning”.

“The brain derives a meaning from chaos, by making sense of and understanding concepts and information through the exploration of a problem domain; all the related success and failures at the subsequent tasks and activities within the exploration help to develop a learner to understand a concept” (Lopez & Alipoon, 2000). The brain naturally integrates and assimilates information while it simultaneously resists the imposition of meaningless patterns (Caine & Caine, 1990). This process may, initially, seem disconnected as the initially isolated information will be related to what makes sense to a particular student. This principle may have the following implications for the education of learners:

- Problem-solving and critical thinking problems can be included in the course material as these are natural activities which encourage the brain to extract patterns (Caine & Caine, 1990; Erlauer, 2003; Sylwester, 1995);
- In terms of “real-life” simulations and activities as principles of brain-based learning, effective learning occurs only through practising and identifying real life applications. Learning is more expressive when the brain supports the processes aimed at finding meaning and patterning;
- Examples of the concept can be provided to the students to help create a clear understanding and to aid them in the creation of patterns and connections between what they already know and the new learning (Tileston, 2004, p. 44);
- Tasks which encourage reflective thinking can be included in the course because they promote learning by encouraging students to analyse their thoughts and experiences and, through reflective thought on the way in which the concepts may apply to or affect themselves, aid them in deriving personal meaning and understanding in both a personal and a global context (Lopez & Alipoon, 2000);
Finally, as an additional aid, this principle encourages allowing the learner sufficient time to process the new information.

### 5.2.6 Every brain simultaneously perceives and creates parts and wholes during the learning process.

"Everything is part of something bigger and is itself made up of parts … The part contains the whole, and the whole, the parts. All knowledge is embedded in other knowledge" (Caine & Caine, 1990, 1991). People learn "by organising new information into hierarchies and organising information so that the relationships between isolated bits of information can be detected" (Banikowski, 1999). Thus, the fifth brain-compatible principle states that *every brain simultaneously perceives and creates parts and wholes during the learning process* (Lombardi, 2008).

The brain has an enormous innate capacity to deal with parts and wholes simultaneously (Caine & Caine, 1991). The brain possesses two generally recognised strategies for organising information. The first method used involves the reduction of information into parts, while the second involves perceiving and working with the information either as a whole or as a series of wholes (Caine et al., 2005). Effective brain-based educational strategies overlook neither strategy but constantly attempt to provide opportunities for students to make connections and integrate parts and wholes.

Successful brain-compatible lessons often engage learners in tasks that require that both sides of the brain, namely, the analytical and the creative (Jensen, 2008c). Cross-disciplinary approaches recognise the importance of including both hemispheres of the brain – the hemisphere concerned with the verbal components and the hemisphere concerned with the visual components of education and communication – in meaningful learning (Lombardi, 2008). This principle may have the following implications for the design and development of an educational approach and its material:

- Concepts would be presented individually and then related to other learnt concepts or contexts.
- Strong visual–verbal (word-picture) associations may be created for new concepts by presenting the work in terms of an associated image or representation in a collaborative manner; for example, providing a picture with its corresponding name or label placed over
the image. This would serve to create a strong association and aid later recall of the concept.

- An initial overview may be provided of the course or lesson plan at the start of the course or lesson. As the course components and lesson tasks are subsequently completed, the learner will then be able to “slot” the newly learnt concepts into their conceptual, global “slots” that were briefly described in the initial overview. This is an extremely beneficial application of the principle as it assists the learner to “build” understanding (Roberts, 2002).

- The purpose (goals and objectives) of each lesson should be presented before beginning a lesson (Banikowski, 1999).

There are many other potential applications of this principle, but the above-mentioned techniques are the most relevant applications for this research study.

5.2.7 It is necessary to review material repetitively to solidify recall and recognition.

Learners should be provided with multiple opportunities and sufficient time to grow their knowledge structures through the practicing and processing of any newly learnt or modified concepts (Smilkstein, 2003, p. 128). Brain researchers are finding that the teaching practices that help students make the greatest gains are not the rote practice drills. Rather it has been found that hands-on learning activities that include discussions, projects, reflection, looking for patterns, enrichment, sharing with peers, comparing and contrasting or problem solving are the most effective education experiences (Caine et al., 2005; Jensen, 2005; Smilkstein, 2003; Wolfe, 2001). Research has shown that reinforcing learning via practice and the application of the higher-level thinking skills positively affects the brain’s long-term memory (Caine et al., 2005; Erlauer, 2003; Jensen, 2005; Jones, 2003; Sprenger, 2003). Thus, the sixth brain-compatible principle states that it is necessary to review material repetitively to solidify recall and recognition.

The purpose of this principle is not that a lesson be covered multiple times in the same format. On the contrary, it suggests that the course material should include the concepts in various forms throughout both the lessons and any further review sessions. Reinforcement activities can include formal, or assistive, assessment, or recreational activities or experiences. Examples of how the “lesson” could be reinforced include exposure to additional expert presentations, supporting notes, repeated or expanded lessons, topic-related games, and so on.
Repeating what has been learnt helps the learner to feel emotionally sure that what has been learnt is true (Jensen, 1995). It is, thus, good practice to encourage learners to reinforce what they have learnt by presenting the material in multiple formats, as recommended by the first principle. This approach is effective because it encourages the learner to consider the concept in a different context from the one in which it was originally taught. This principle has the advantage of promoting active processing of an experience through the analysis and synthesis of ongoing changes and experiences in order to construct, elaborate and consolidate mental models (Gülpinar, 2005). This principle has the following implications for the development and implementation of an educational effort:

- Multiple activities, which each approach the concept in a different way, may be included, for example discussions, assignments, quizzes, polls, games, etc. The reason this approach may be effective is because the human brain likes interesting activities, relevant knowledge, and choices. When people are allowed to make choices, for example select the method of education to which they will subscribe, interest, motivation and effort are all increased while stress is decreased (Banikowski, 1999; Erlauer, 2003).
- Questions and mini-activities which encourage the reviewing of concepts may be included throughout the activities and materials of the education efforts. This is done in order to encourage learners to understand and retain the information they have been taught. In addition, time for reflection during every lesson will allow the learners’ brains to develop meaning and personal relevance from the concepts introduced (Jones, 2003).
- Hands-on activities may be included in order to assist with the thorough exploration of the new concepts as this will allow abstract concepts to become concrete for the learners (Caine et al., 2005; Erlauer, 2003; Jensen, 2008c; Smilkstein, 2003; Sprenger, 2003; Wolfe, 2001).

There are many other potential applications of this principle to course material but the above mentioned are the most practical for online applications. Several applications of the principle are recommended. Erlauer’s research shows that, after four practice sessions, students will reach a competence level of 47,9% of complete mastery of a skill or concept. It will take the students 20 more practice sessions, a total of approximately 24 times, to reach 80% competency. For storage in long-term memory, it is therefore better to learn a few concepts extremely thoroughly rather than several concepts in a vague way (Erlauer, 2003, p. 82).
5.2.8 Both the focused and peripheral attention of a learner should be involved in the learning process.

The seventh brain-compatible principle focuses on involving both the focused attention and the peripheral attention of the learner in the learning process. Learning always involves conscious thought and focus but, as a result of unconscious processes, during learning most of the signals that learners perceive peripherally also enter the brain (Caine & Caine, 1990).

The findings of brain-based researchers indicate that over half of what a learner learns does not come from what the teacher is saying but rather from the surrounding environment (Erlauer, 2003; Jensen, 1995). This is because learners have a limited attention span and they tend to lose focus sporadically during prolonged lessons. During these periods of unfocused attention, their peripheral interest and attention may be engaged by their surroundings and environment. The brain learns both consciously and para-consciously, through nonverbal communication, voice and physical environment, with that learning engaging the entire physiology (Lombardi, 2008). This means that while the brain absorbs the information which a learner is paying direct attention to, it also absorbs information and signals that lie beyond the learner's immediate focus of attention.

This finding indicates that learners will remember not just what they are told but also what they experience (Caine & Caine, 1990). O'Keefe and Nadel (1978, as cited by Caine & Caine, 1990) explain that “the brain responds to the entire context in which teaching or communication occurs”. “Every sound, every visual signal is packed full of complex meanings and impact on learning” (Caine & Caine, 1990). Therefore, it is essential that educational efforts communicate or teach their content in such a way that the learners’ direct and peripheral attention is focused on the educational material or experience. Possible applications of this principle for an educational effort could include the following:

- Tasks which allow learners to explore concepts in relation to themselves should be included in the education effort. Learners should be allowed to review how and what they learnt at their own leisure. This enables them to take charge of both their own learning and the development of their own personal meanings for the concept and its related information (Lombardi, 2008). Examples of tasks could include activities which require the learners to explain or demonstrate to themselves or other learners how a concept applies to themselves or a familiar situation.
Chapter 5 Theoretical Basis Used in Action Research Interventions

- Reflection and meta-cognitive activities may be included, for example question-and-answer sessions, evaluations, tasks requiring reflection or the demonstration of understanding.

- Elaborate procedures and theories should be explained using metaphors and analogies in order to help students to recognise and relate to the material in a personally valuable way (Caine & Caine, 1990).

- In order to engage the peripheral attention, information may be organised in such a way as to ensure that learning includes peripheral visuals, for example charts, illustrations, videos, set designs, art and the use of music to enhance and influence the more natural acquisition of information (Caine & Caine, 1990).

- Colours may be used to manipulate the learner’s emotions and focus, as well as to direct attention, for readability and to improve comprehension. For example, yellow is the first colour to be distinguished by the brain and is excellent in an educational environment or materials. Taylor quotes Deborah Sharpe and Faber Birrin as stating that colours such as yellow, which elicit positive moods, and green, which encourages both productivity and long-term energy, are effective in classrooms (Taylor, 2007). Blue is acknowledged as creating a relaxing learning environment.

On a fundamental level this principle relies on the ability of the learner’s brain to absorb direct information and “fringe thoughts”. The mind perceives subtleties and, frequently, the subtext of a speech and the nuances of a situation may affect attention, perception and learning through unconscious processes (Lombardi, 2008). By focusing both forms of attention, the learner’s degree of understanding and memory of the relationships between conceptual components may improve and strengthen.

**5.2.9 Allow learners to progress through the course at their own pace.**

People learn at different rates and, thus, this eighth and final principle involves allowing learners to progress through the course at their own pace. Learners need to be encouraged to participate actively in the learning process. This principle is highly appropriate for enabling learners to take control of their own learning and to adjust it to suit their own personal needs. It gives the learners the freedom to progress through the course material at a pace which is compatible with their own concentration span, study methods and processing rate. Allowing learners to progress at their own pace improves their chances of completing the course successfully. In terms of cybersecurity
education, it provides learners with the opportunity to acquire the desired cybersecurity and safety awareness, knowledge and/or skills in a flexible manner.

A note of caution is sounded for this principle, however; although the learners may progress at their own pace they should not be provided with an infinite amount of time to complete a task. A final completion deadline is still required as a motivator for students who may never complete the task should they be left to their own devices with an infinite amount of time in which they may or may not complete a task. In brief, what this principle actually recommends is that learners be allowed to progress at their own pace through tasks and course material within a specified amount of allotted time. Possible application of this principle to an educational effort may include the following:

- Students should be presented with lessons and tasks (for reinforcement or assessment) and given a final due date for submission.
- Students could be allowed to chart their progress and measure their success (Futa & Gocłowska, 2005). Methods for doing this could include the use of mark sheets or logs in formal education activities, or discussions and answering of questions for talks, or taking turns in games etc. Any method which allows learners to reflect on what they are capable of after completing the lesson compared with what they were capable of before the lesson would be suitable (S. Rogers & Renard, 1999).
- A “leader board” or “winners and runners-up” may be included to encourage competitive progression.

This principle is governed by both time management and freedom of choice and there is much reliance on the ability of students to manage their own learning experience and to perceive their own capabilities and limits. However, some guidance is necessary in order to guarantee an end to the activities.

This concludes the discussion on brain-compatible pedagogy and its principles (section 5.2). The next section will discuss active audience theory, which was used during the Cycle 4 of the action research process presented in Chapter 11. The BCE compliance of the cybersecurity education campaign presented in Chapter 6 to Chapter 11 was used to try to optimise the way in which the cybersecurity messages were communicated to the learners. Active audience theory was used to attempt to determine whether the audience understood the message as it was intended.
Chapter 5 Theoretical Basis Used in Action Research Interventions

5.3 Active Audience Theory

Cultural studies and media studies have been co-developing for several years. Media, particularly television, has been a major form of communication in most western societies (and worldwide) (Barker, 2012).

Television and media are increasingly available resources for communicating messages to audiences via their programmes, namely, news, documentaries, and fictional series, among others. They are implicated in the provision and the selective construction of social knowledge and social imagery, through which audience members perceive “worlds”, the “lived realities” of others, and imaginatively reconstruct their lives to render them intelligible and to create an understanding of a “whole-of-the-whole” (Barker, 2012; Hall, 1977). Understanding this communication and cultural process requires the consideration of many dimensions and perspectives.

One perspective examines the relationship between texts and audiences (Barker, 2012). This perspective is categorised as audience research. There are many audience-related research areas, one of which is the audience’s role in the “consumption” and processing of media messages or texts. One area of audience research that is of interest, and has relevancy for this thesis, is the active audience paradigm.

The active audience paradigm suggests that it should not be assumed that audiences develop a culture by uncritically accepting the “textual” meaning of a programme (Barker, 2012). Audiences can be passive consumers or active consumers. Accordingly, there are a number of models that address both theoretical stances: a passive audience model assumes that a text shared by the media will have a direct, predictable influence on a passive audience, while an active audience model on the other hand suggests that audiences interact with the text and actively create meaning from it based in their own cultural context (Barker, 2012).

Active audience theory examines the active, interpretative role of an audience when members of that audience “make meaning” from the media content based on their own cultural context (Hall, 1981; Munday & Chandler, 2011). The theory argues that media audiences do not just receive information passively but are actively involved, often unconsciously, in making sense of the message within their personal and social contexts (Munday & Chandler, 2011). This means that each audience member’s interpretation and acceptance of intended messages may be influenced
by considerations such as family background, beliefs, values, culture, interests, education, and experiences.

Another consideration in the process is that “texts” are polysemic. They can be ambiguous and carry multiple meanings. This polysemic nature of messages is not necessarily intentional. Only some of the meanings will be taken up by audiences and which meanings are adopted and who adopts them can depend on the number of textual meanings and the particular audience.

Existing research has drawn a number of conclusions about active audiences in the context of television and media. These conclusions, as given by Barker (2012), are as follows:

- The audience is acknowledged as acting as knowledgeable, active producers of meaning, not products of a structured text.

But ...

- The audiences need to be understood in the context in which they view the media in terms of meaning construction and the routines of life.
- Audiences are capable of differentiating between fiction and reality. They are also capable of actively challenging the boundaries between the two.
- The process of meaning construction and the place of the media in daily life alter from culture to culture and in terms of gender and class within the same cultural community. This research will not examine gender and class difference when applying the theory; however, it will be showing differences between cultural groups. For the purpose of this research different culture groups will refer to learners from different schools. The assumption being that distinct cultures form amongst audiences in different contexts. Overall the cultures may be similar however their intricacies may vary.

The active audience paradigm and its conclusions about active audiences have been reached through various theoretical and empirical research works. Theoretically, the paradigm has been significantly informed by the encoding/decoding model of communication. It is this model that enables the further understanding and application of active audience theory. Future references to active audience theory in forthcoming chapters will make use of the encoding–decoding model. The next section will examine this model.
5.3.1 Encoding–decoding

Stuart Hall’s encoding/decoding model suggests that an active audience has to decode the meanings within a text, therefore different audiences will do so in different ways (Hall, 1981). A number of factors will influence the way the audience interprets the text.

Audiences may interpret meanings from messages based on their own previously acquired cultural competencies, which they produce in the context of language and social relationships. This means that every member of an audience will have their contextual influences when they interpret a meaning from a message.

For the purpose of the encoding/decoding model an audience is considered to be a group of socially situated individuals whose “reading” of the “text” will be framed by shared cultural meanings and practices.

The aim of a media “text” is typically to communicate a message with a specific meaning. Stuart Hall examined the process of communicating and interpreting the meaning of messages as “text” in the “conversation” between the “text” creator and the target audience. This was resulted in the visualisation of the process of communication.

The process of communication consists of a circuit comprising a complex structure of relations. Hall (1981) visualises this process in terms of television encoding as the articulation of the linked but distinct moments in a circuit of meaning (Figure 5.1). The circuit includes stages for the production, distribution, circulation and reproduction of a message (Hall, 1981). In this circuit the “sender” of the message has become a “producer” and the “receiver” of the message is a “consumer” (Procter, 2004, p. 61).

![Figure 5.1 Hall's (1981) “circuit of television”](image-url)
Within this circuit of communication, messages are sent between stages or parties. Typically, the message has a meaning that the sender tries to convey when constructing and producing the message. However, as the message moves within the circuit, it is not guaranteed that each level will interpret (consume) the meaning of the message similarly or even at all. This is because the meaning of a message is polysemic (can intentionally or unintentionally have multiple meanings) and an audience can interpret these meanings in different ways. Stuart Hall’s encoding/decoding model (see Figure 5.2) illustrates this by showing the transmission of the meaning of the text between its producer (encoder) and the reader (encoder) (Hall, 1981).

![Encoding and decoding of broadcast structures (Hall 1980)](image)

Figure 5.2: Encoding and decoding of broadcast structures (Hall 1980)

Hall argues that media has a preferred message to communicate to its audience. The text of the preferred message would be structured and presented in a “dominance” encoding position to lead the audience to the preferred meaning (Barker, 2012; Hall, 1981). However, this does not guarantee the consumption of the encoder’s preferred meaning by the audience, as audiences do not passively accept information and its imposed meanings from a structured “text” (Munday & Chandler, 2011; Procter, 2004, p. 69).

Within the circuit of communication the encoding/decoding model shows that audiences are active and knowledgeable producers of the meaning of a text’s delivered message within their own personal and social contexts (Barker, 2012). The producer (encoder) encodes meaning in a certain way, while the reader (decoder) decodes it differently according to their own personal knowledge and contextual frames of interpretation. It cannot be assumed that the meaning of a programme, text or any other communication has a fixed interpretable meaning that can
unerringly be recognised by any audience. Instead, the way the audience makes sense of a text’s meaning is “the product of a negotiation between the audience and the text in a particular context of reception” (Munday & Chandler, 2011).

The audience and the producers/encoders of a message are expected to share the interpreted meaning position to the same degree as they share cultural codes (Barker, 2012). To increase the amount of shared meanings it is therefore very important when developing material or communicating a message that it be developed or communicated so as to apply and leverage similar or shared socially situated knowledge and practices in the communication of the messages.

In brief, different audiences (and the encoders) may accept different textual meanings based on how the text is constructed and communicated, and based on their contextual cultural influences. Texts (the messages) are polysemic (can have multiple meanings) (Hall, 1981). Often only some of the meanings will be accepted by an audience (Barker, 2012). The audience’s decoding will typically fall into one of the following three hypothetical decoding positions within cultural contexts, as proposed by Hall:

- **The “dominant-hegemonic encoding/decoding” position**

  Within this decoding position the decoder accepts the message’s “preferred meanings”, which a text is attempting to impose (Hall, 1981). Often this position is adopted as the text reflects the ideas and beliefs of the audience, for example the subject matter may be the reason or relate strongly to a reason the audience member is interested in the matter or it may affect their life or activities to some degree. Within this position there is little misunderstanding and miscommunication. This is often attributed to the sender and the receiver working under the same rule set, assumptions, and cultural biases.

- **A “negotiated code” position**

  Within this decoding position the decoder acknowledges the legitimacy of the theory of the hegemonic decoding, but adapts its interpretation based on a particular context or circumstances (Hall, 1981). This position is adopted when an audience member largely understands the meaning of the text, but in a different sense from the dominant-hegemonic viewpoint. An example of this position could have the audience member acknowledging the importance of a concept, but the message could also be deciphered as being more personal, which means it will be influenced by
their biases and viewpoints. This could confuse or alter the way in which the message was meant to be interpreted, without causing the message to be rejected.

- **An “oppositional code” position**

Within this decoding position audience members understand the preferred encoding, but they reject it and decode the text in a conflicting way (Hall, 1981). In terms of this position, the audience member is capable of decoding the message in the way it was intended but, based on their own societal beliefs, often sees an unintended alternative meaning. In taking this position, an audience member consciously rejects the preferred meaning and relates to an opposing view. For example, the text’s message provides positive information about a particular issue, but the audience relates more to the negatives of the same issue.

All positions are the result of the entire communication process and the audience members’ decoding of the text in order to produce their own *new meaning* of the message for themselves. In this production of new meaning, the text may structure aspects of the meaning by guiding the reader; however, it is important to note that the text cannot fix interpreted meanings which are the outcome of misinterpretation resulting from target audience members’ misunderstandings or incorrect inferences (Barker, 2012).

This concludes the discussion of active audience theory and the encoding–decoding model (section 5.3). This contextual theory was applied in Cycle 4 of the action research process presented in Chapter 11. This section is the last section to present relevant literature for the action research process, Chapter 6 to Chapter 11.

### 5.4 Conclusion

This chapter examined brain-compatible education and the active audience paradigm. Theory on brain-compatible education was the first theory to be examined. As a pedagogy, brain-compatible education can be used to influence the learning experience and its effectiveness. Eight brain-compatible principles, which were considered most relevant to this work, were outlined, and discussed. In addition, some suggestions from the literature for the practical application of the principles were also provided. The pedagogy has been applied with considerable success in various classroom setting worldwide and its application has been acknowledged as being beneficial to learners and their general learning experiences. The second theoretical consideration to be discussed was the active audience paradigm. This paradigm examines the
relationship between media “text” and its intended audience. It describes how audiences are not passive in accepting the intended media message, but rather interpret it actively. The process of communication from the encoding of the message by the media to the decoding of message by the audience was briefly described. Three hypothetical decoding positions, as proposed by Hall (1980), were discussed in terms of television programmes and their audiences. The next chapter will examine how the abovementioned theories were applied in the various action research cycles.
6 Action Research Process

“It is common sense to take a method and try it. If it fails, admit it frankly and try another. But above all, try something.”

~ Franklin Delano Roosevelt
This chapter presents the discussion and analysis of the action research process. This consists of five iterative cycles. In order to meet RO3 of the thesis, the action research process investigated factors within a cybersecurity awareness and education campaign that might contribute to the success of education efforts targeted at school children. This chapter presents the practical implementation of the action research process. Chapter 5 presented the overviews of the theoretical basis underlying interventions within the research cycles.

6.1 Introduction

Earlier chapters have shown that education is an important contributor to the raising of cybersecurity awareness amongst users. Conceptually, a culture of cybersecurity is not easy to describe. A culture is a highly contextual construct. Cybersecurity education is thus similarly influenced by the context. The environment, target audience, activities, and other pre-existing cultures will affect the design, implementation, and impact of the cybersecurity education campaign.

Chapter 2 and Chapter 3 showed that education campaigns or efforts could contribute to educating broader society about cybersecurity. Chapter 3 discussed the practical part of the study, the focus on educating the youth about cybersecurity. In this study, “youth” refers to children who are enrolled in a formal education system, i.e. school children or learners. RQ3 of this study is “What effect do various cybersecurity and cybersafety educational interventions have on school children’s cybersecurity and cybersafety knowledge?” This chapter aims to answer this question.

The researcher conducted a cybersecurity campaign that was aimed at educating school learners about cybersecurity and cybersafety. Several factors (issues or considerations) affecting the campaign were taken into account. These issues were identified from literature studies, and from the researcher’s experience of working with this campaign. An action research strategy was used to guide the examination of the selected issues.

6.2 The Action Research Process: Overview

Fundamentally, action research is a collection of sequential problem-solving processes. An action research process involves iterative cycles of:
Chapter 6 Action Research Process

- identifying a problem or idea
- considering and planning a potential solution
- implementing the plan
- measuring and analysing the results of the action taken, and finally
- reflecting on the lessons learnt from the process.

The lessons learnt may aid in re-evaluating the problem or idea under consideration, and this may result in another cycle. This is the implementation of the age-old education principle of learning via experience ("learning by doing"). The purpose of this chapter is to report on the action research process conducted during a cybersecurity campaign.

Reporting on action research is a challenging endeavour as it requires writing for two audiences, academics, and practitioners. In order to disseminate the action research effectively, Somekh (1995) recommended the production of a single, long report for both audiences and a number of short discussion documents targeted at specific groups. Action research reports are often narratives, located in the context of the evolving experiences of those involved (Heikkkkinen, Huttunen, & Syrjälä, 2007). Because the research design can be very complex, reporting the findings requires a well-organised narrative, clear writing style, and precise word choice.

Chapter 5 and Chapter 6 to Chapter 11 collectively form the single long report for both audiences. Several publications then serve as the reports for specific target audiences. Section 4.3 discussed each publication that stemmed from this research. The publication to which data were contributed are also noted in each research cycle.

During the research process, findings were published using the data available at the time of publication of journal articles (Appendix A) and conference papers (Appendix B). However, in some cases additional data have been gathered via late submissions or further access to target audiences. For the purposes of the final analyses presented here, all data as of June 2016 were included. Therefore, some results may differ slightly from the corresponding earlier publication.

The next section discusses the broad context of the action research process. The target audience of the campaign are discussed within the broad context the SACSAA campaign.

6.3 Broad Context

Action research facilitates change by emphasising action. It achieves this by enabling researchers not only to suggest appropriate lines of action, but also to investigate the actual effects of the
actions. This study investigates factors and issues within and surrounding cybersecurity education campaigns that target broad audiences. Ideally, cybersecurity education campaigns should target all users in a particular society. As a result of challenges in scope, however, the practical actions taken within this study were only taken in a cybersecurity education campaign targeted at school children (as discussed in section 1.5).

This section will discuss the action research process conducted whilst working with the annual South African Cybersecurity Academic Alliance (SACSAA) cybersecurity education campaign. The next section discusses the parameters and target audience of this campaign.

6.3.1 The SACSAA Cybersecurity Education Campaign

The South African Cybersecurity Academic Alliance (SACSAA) is an alliance of academic research groups from Nelson Mandela Metropolitan University (NMMU), the University of Johannesburg (UJ) and the University of South Africa (UNISA) (SACSAA, 2011). The alliance was established in June 2011 (Elmarie Kritzinger, 2011). Its main goal is to communicate with the public about current cybersecurity issues, knowledge, and practices.

In meeting this objective, the main activity of the alliance members is campaigning for the effective delivery of Cybersecurity Awareness to all members of the population of South Africa (SACSAA, 2011). Each of the founding institutions is committed to conducting at least one cybersecurity awareness activity per year. The focus of this study is the cybersecurity educational campaign and competition run by researchers from NMMU.

The NMMU campaign and competition runs annually in the months preceding the national cybersecurity week. It concludes with a closing event and a competition awards ceremony during cybersecurity awareness week.

The NMMU researchers began running the SACSAA awareness and education campaign in 2011, when they conducted a pilot study for such a campaign. The campaign discussed here focused on South African school children as its target audience. Eventually it will target all members of society. Section 6.3.2 discusses the target audience in more detail.

The SACSAA campaign itself consists of two parts: an education campaign and a poster competition.
Humans are among the assets and role-players in cybersecurity solutions. The campaign aims first to raise the school learner’s awareness of several important cybersecurity and cybersafety topics specific to the practice of cybersecurity. There are seven main thematic messages in the campaign. These themes include topics that cover those issues acknowledged as being most relevant to common cyber activities. Each year’s campaign covers a wide variety of cybersecurity and safety topics within these themes. The seven messages in this campaign and examples of topics within these themes are:

- **Keep your private information private**
  This theme placed emphasis on learners not sharing their own, or someone else’s, personal information, or password with anyone besides their parents. Scenarios such as posting information on online profiles or chats, or sharing passwords with friends were explained as risky practices. Numerous threats posed by others using this information to target or impersonate the learner were explained, e.g. identity theft. Topics often covered in this theme include information security, social networking, cyber identity management, and general browsing or downloading.

- **Have a secure password**
  This theme covered the importance of securing profiles and accounts against threats with a password or similar security mechanism. How to create, remember and manage passwords was covered.

- **Be nice online**
  This focused on messages encouraging learners to avoid being bullies, and to report bullying if they saw it happening online or in communications between peers. Various forms of cyberbullying, how to identify them and how to prevent or report them were covered. This topic also covered contributions to online communities such as commenting, blogging, creating online tutorials etc. Topics covered within this theme included cyberbullying, -citizenship, -harassment and -stalking, and general online browsing, cyber identity management, and social networking.

- **Stay legal**
  This theme focused on teaching learners to avoid illegal activities such as online piracy of any copyright material, or eliciting other people’s confidential information for any reason, including illegal or malicious reasons. It also discouraged learners from visiting sites or
downloaded content that contained illegal content or was linked to illegal activities. Topics covered in this theme included online piracy, social networking, and cybercrime.

- Trust an adult
  This theme focused on learners’ need to trust a parent, guardian, or adult and to report instances of dangerous, harmful, or threatening online activities. This theme was linked to all the topics, but most especially to cyber-bullying.

- Protect your PC
  This theme focused on the importance of learners protecting their computers or other devices against threats targeted at these devices, or at the information they contained. Topics covered in this theme included password security, preventing viruses and malware, and avoiding physical threats such as theft.

- Stranger Danger
  This theme focused on how befriending strangers online was similar to but even more dangerous than befriending someone on the street. The ways in which people can misrepresent themselves online was covered in depth. Related issues such as grooming, catfishing, child predators, and social engineers were covered in this theme. Other topics included cyber-bullying, harassment, and stalking.

The ensuing sections of the chapter focus on the topics identified in learners’ posters.

6.3.1.2 The Poster Competition

The poster competition is an instrument used to measure the campaign’s impact on school learners’ awareness levels. Learners are invited to create and submit posters that promote awareness of security issues covered in the campaign. Posters may be hand-crafted or digitally-created. In order to incentivise participation, prizes are offered each year. A panel of judges from the School of ICT selects the winners using a majority vote. They take into consideration the accuracy of the poster’s content, its artistic presentation, and the overall impact of its message.

From a research perspective, the posters serve as sources of data. After each research cycle, all posters received that year undergo a thorough qualitative content analysis to measure the effect of the campaign. The action planning measurement section of each research cycle outlines the focus of each year’s analysis.
The content analyses are conducted as described by Krippendorff (2004). A content analysis can be conducted on any texts or artefacts (Hodder, 1994). A text is “anything that has meaning to somebody, including the analyst, and can be examined or read repeatedly” (Krippendorff, 2013, p. 389). Examples include letters, e-mails, blogs, literature, images, video, photographic images, posters, cultural artefacts and so on (Krippendorff, 2013, p. 389).

In this case, the posters are interpreted artefacts, illustrating how each learner interpreted and understood the cybersecurity campaign’s messages. The researcher believes that the results of such poster analysis provides information about the campaign’s contribution in encouraging the creation of a cybersecurity culture among its target audience.

The SACSAA campaign was used as a case study in each of the action research cycles: the effect of the interventions was assessed, and data were collected for analysis. The campaign issues and the processes used to address them are discussed according to the campaign cycles in which they were introduced.

### 6.3.2 Target Audience

As previously discussed, all members of our current information society would benefit from gaining some level of cybersecurity awareness and related secure behaviours (section 2.2). The ideal target audience for a cybersecurity campaign is therefore all cyber citizens within a society. It was not possible for the researcher to conduct a practical study focusing on such a wide and diverse audience. Section 2.6 acknowledged this challenge, and a decision was made to scope the practical part of the study to focus on school learners.

The typical target audience for cybersecurity education is diverse, geographically dispersed and made up of individuals who have many diverse characteristics, needs and abilities. Characteristics of importance include age, abilities, background, culture, etc. Needs include organisational role, private role, basic knowledge, advanced knowledge, etc. Abilities include lack of or level of prior formal training or self-education. These characteristics would be present in almost any target audience in a broad societal context, including the selected target audience of school learners used in this research study.

The SACSAA awareness and education campaign was selected as the case in the action research process. The current SACSAA awareness and education campaign, run by the NMMU researchers within the alliance, has South African school children as its target audience. A pilot
study of the SACSAA campaign was implemented in the Nelson Mandela Metropolitan Bay area in 2011, and is still running. The target audience is therefore school children in the Nelson Mandela Metropolitan area.

This target audience was a convenient and purposive sample for analysis in this study. Firstly, it is a convenience sample as the data was "available to the researcher by means of its accessibility" (Bryman, 2012). The researchers had been gathering data for several successive years for research purposes. Secondly, this sample is also purposive as the sample participants were specifically selected "so that those sampled are relevant to the research questions that are being posed" (Bryman, 2012).

Initially the campaign intended to target all school children and university students by conducting awareness and education activities at various educational facilities in the area. However, after the “trial run” of the campaign in 2011, the target audience was refined to include only primary school children and high school learners.

In 2011, the campaigns first attempt targeted NMMU students, high school learners and primary school learners. This campaign was conducted following a basic version of the campaign effort format presented in section 6.3.1.

In 2012, the SACSAA campaign opted to take a different approach to targeting university students. Thus, from 2012 onwards, the SACSAA campaign of awareness activities and poster competition included only primary school and high school learners.

In 2014, a curriculum developed by Von Solms and Von Solms (2014) was adopted for use in the campaign. This curriculum was designed for school children. Based on this and other factors described in the cycle (section 6.4.4.2.1), the target audience for the campaign was refined a final time, focusing on primary school learners only (Grade R – Grade 7). This audience did not change in 2015.

The campaign aims to give a robust foundational knowledge in terms of cybersecurity to learners at an early age. Therefore, most of its activities are designed for this age group. The campaign does, however, continue to target the high school learners in order to reinforce and update existing cybersecurity knowledge and behaviours.

Since the campaign’s first implementation, many schools have taken part, although only one has participated in every iteration of the campaign. This school is referred to as School A, and is the only school to have been exposed to all changes to the SACSAA campaign.
Amongst the other schools, several have taken part in multiple iterations, and some have only taken part once. These schools did not experience all the changes. Therefore, to show the impact of these changes, the analysis of results will focus primarily on School A’s data as it is the most complete data set. However, it will also present the results and findings from the other schools when they are available.

The samples are believed to be representative of the SACSAA campaign’s general target audience. The primary school subgroup had an age range of between 6 and 15. The high school participants had an age range of between 14 and 18. Members of both genders and different ethnic groups were represented in both age groups.

Research ethics considerations resulted in no identifying data apart from participant age and school attended being captured. The names of the participating schools were anonymised.

Table 6.1 shows school participation per year for the four official campaign cycles (2012 to 2015). High school participation was not sought in the 2014 and 2015 iterations.

<table>
<thead>
<tr>
<th>Anonymized Name</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Schools</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>School A</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>School B</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>School C</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>School D</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>School E</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>School F</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>School G</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td><strong>High Schools</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>School AA</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>School BB</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>School CC</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

The next section describes the action research process cycles.
6.4 Action Research Cycles

The action research cycles are presented in chronological order. The campaign began with the pilot year, 2011, and concluded with the final fully completed cycle year, 2015. In each cycle, each phase of an action research cycle was addressed according to Susman (1983), namely:

- Problem Identification
- Action Planning
- Implementation
- Results and Evaluation
- Reflection

Figure 6.1 shows how the phases relate to one another. The reflection phase of each cycle can affect the following cycle’s problem identification.

Figure 6:1 Action Research Model (Adapted from Susman (1983))

- **Problem Identification**

  The first phase involves the identification of the problem to be addressed (Susman, 1983). In this case, this is the identification of factors that affect educational efforts which aim to raise awareness and educate broader society about cybersecurity. Each cycle within this section identifies the issues or factors that have an impact on the effectiveness of the SACSAA
campaign, and which are then discussed in the iteration. Some of the issues were identified in the literature, whilst others were identified in preceding action research cycles.

• **Action Planning**

The second phase consists of the suggestion of a possible solution to the problem, and the creation of a relevant "plan of action" (Susman, 1983). Each cycle in this section provides a discussion of a potential solution to the identified SACSAA campaign issue. Literature was consulted when necessary. Chapter 5 discussed the relevant theoretical basis of some of the solutions that are provided in Chapter 6 to Chapter 11. Chapter 5 presented the theoretical literature separately, as some of the actions taken within multiple iterations shared a theoretical basis. Where applicable, the measurements, and the relevant instruments used to gather these measurements, are discussed in this phase.

• **Implementation**

The third phase consists of the actual implementation of the plan (Susman, 1983). In this third phase, data are collected for future analysis and evaluation of the action taken. Each cycle in this section describes the actual implementation of the SACSAA campaign in a particular year.

• **Results and Evaluation**

The fourth phase involves a thorough analysis of the collected data, and the consequences of the actions taken are studied (Susman, 1983). Each cycle presents the iteration’s results and an analysis of the results of the annual SACSAA cybersecurity education campaign. The results are discussed according to two categories.

  o **School A**

    The two categories related to how consistently schools had participated and submitted posters. The first category represents the results pertaining to School A. School A was the only school that took part in all aspects of the campaign in all official campaign cycles (2012–2015). These results are presented as a separate ongoing study to indicate how consistent and recommended campaign implementation might affect a target audience. This category represents the results of a full implementation of the recommended campaign plan and procedures.

  o **Other Schools**

    The second category comprises the results of other schools participating in the campaign, where applicable. These schools took part inconsistently or changed
implementation procedures. The researcher believes these results would be typical of a campaign with many participants and varied implementations.

• Reflection

The fifth and final phase within the cycle involves reflection. In this phase, the findings of the cycle are interpreted in terms of the success of a particular action, and the problem is re-assessed (Susman, 1983). This concludes the cycle, and the next cycle then begins.

The process is repeated until the problem has been resolved. Each cycle in this section outlines the general lessons learnt from the iteration’s action. Particular concerns or issues identified as a result of the iteration are also be outlined. Subsequent iterations then address some of the outlined issues.

Multiple issues arose in each iteration. Some issues were addressed over the span of multiple campaign iterations. When issues spanned multiple cycles, their earlier data was considered in later cycles.

Each action research cycle is linked to the next by the results and of the critical reflection on lessons learnt in the cycle. The reflection often results in the use of conceptual tools in planning the next actions. As the research progressed through the cycles in this study, a process of refining methods, adjusting decisions about data collection and evolving strategies for data interpretation was ongoing. The iterations discussed in the following subsections are illustrated in Figure 6.2. Lessons learnt during the iterations influenced subsequent iterations and the overall lessons learned.

The lessons learned, and actionable knowledge gained from the entire action research process are presented and discussed throughout the reflections sections of each research cycle (Chapters 7 to Chapter 11).
Chapter 6 Action Research Process

Figure 6.2 Action research cycles from 2011 until 2015
6.5 Conclusion

This chapter provided an overview of the action research process. Then it presented the broad context and target audience of the SACSAA cybersecurity and cybersafety educational campaign. This campaign was designed, implemented, modified, and analysed during the action research process. General details and procedures as there were applicable to all of the action research cycles were discussed. Chapters 7 to Chapter 11 discuss the individual action research cycles in detail.
Chapter 7 Cycle 0: Pilot

“The beginning is the most important part of the work”

~ Plato
This chapter provides an overview of the research process followed during Cycle 0 of the SACSAA cybersecurity and safety campaign.

7.1 Introduction

The very first iteration of the SACSAA campaign was implemented in 2011. Cycle 0 of the campaign served as a “trial run” of the cybersecurity and awareness campaign. The researcher joined the campaign effort during the reflection phase of Cycle 0. The iteration is discussed according to the outline shown in Figure 6.2. This was the first iteration of five action research cycles and campaign years included in the thesis.

7.2 Problem Identification

As discussed in Chapter 2 and Section 6.3.2, there exists a need to educate the youth about cyber-security and cyber-safety. The SACSAA campaign aims to reach all South African school learners and university students. However, the implemented campaign addressed in this thesis is the “pilot study” within the Nelson Mandela Metropole. The objective of the campaign is to, at the least, raise the target audience’s basic levels of cybersecurity and cybersafety awareness, which they need daily. The ideological aim of the campaign is to contribute to the fostering of a cybersecurity culture amongst members of the target audience by raising their knowledge (awareness), and potentially influencing their behaviour.

Cycle 0 of the campaign was a “trial run”. The trial run was necessary to establish a baseline for the campaign’s implementation and effectiveness. This campaign cycle would be used as a starting point of comparison with future iterations.

The campaign needed to meet two criteria. Firstly, it would need to contain an awareness, training or education component which targeted school learners. The Cycle 0 – Objective 1 (C0O1) was: to provide this educational component.

Secondly, the effect the campaign had on learners should be measurable in some way. Cycle 0 – Objective 2 (C0O2) was thus: to provide a method of evaluating the campaign’s effect on the learner.

The next section outlines and discusses the “plan of action” followed in the 2011 campaign.
7.3 Action planning

This campaign iteration was intended to establish a baseline, and to start the initiative of educating school learners about cybersecurity and cyber-safety. The basic implementation for computer security awareness and training course was planned (NIST 800-12, 2004), from identifying a goal to evaluating the campaign.

The SACSAA campaign aimed to target all children and young adults (target audience). Ideally, all users within this younger age group would be educated about cybersecurity and safety (goal). However, reaching children in a home environment presented challenges to implementation that could not be addressed by the researcher. A decision was made to target children and young adults who were enrolled in formal education at schools and universities (target audience context). This decision was made to take advantage of the existing educational processes and resources, and to ensure access to the right target audience.

Cycle 0 targeted and invited participation from learners at primary schools, high schools, and the NMMU.

SACSAA was established in June 2011 and this campaign iteration was run shortly after its establishment. As a result, the campaign ran in the third term of the school year.

The campaign required two components namely: an awareness-raising or educational effort, and a method for measuring the effect or result of that effort. The research group decided to implement a cybersecurity poster and video competition, the purpose of which was to be both educational and a method of gathering data to measure the campaign’s effect. It would fulfil its purpose in each role as follows:

- **The educational effort**

  The competition made a call for participants to enter creative and educational videos and posters on cybersecurity. Examples of topics were included on the poster, alongside campaign representative contact information where users could obtain further suggestions. Suggested topics included phishing, identity theft, social networking, cyberbullying, and malware.

  The competition was intended to be run as a distance learning initiative, where learners engaged in independent study. The aim was to raise participants’ awareness by encouraging them to educate themselves in the cybersecurity topics they intended to
include in their posters or videos. Winning material was expected to be included in future awareness-raising exercises.

- **Data Collection**

  The competition was designed as a means of gathering data to measure the effect of the educational component. It was expected that entries in the form of posters and videos would be received. These entries would reflect participants’ understanding of topics. It was hoped that analysis of these entries would contribute to measuring the effect of the educational effort. The measurements for analysis were:

  - **Learner participation**
    Measuring the number of participants would indicate how many learners were affected by the competition. Participation of learners from the invited schools and university was expected to be voluntary. Participation could provide an indication of learners’ interest in the campaign and/or the effectiveness of the campaign’s implementation approach.

  - **Posters per topic**
    The purpose of measuring which topics were explored by learners was to indicate which topics learners considered a priority or to which they related most strongly.

SACSAA advertised the competition using professionally designed flyers, as illustrated in figure 7.1. These flyers were distributed to all schools in the Nelson Mandela Metropole via post. Flyers were also displayed on several NMMU campus noticeboards. Finally, the flyer was posted on the NMMU research group’s SACSAA website (www.cyberaware.org.za).
The competition comprised categories for primary school learners, high school learners, and university students. Participation was completely voluntary. Generous cash prizes were offered to motivate learners and students to take part. The overall winner would receive R1000, the first runner-up R300 and the second runner up, R100. These prizes were intended to act as incentives to attract learners to participate.

7.4 Implementation

The campaign was implemented as planned. The campaign’s poster competition was advertised using the flyer (Figure 7.1). These flyers were distributed via the post to several schools in the Nelson Mandela Metropole together with an official letter of invitation to participate from the
NMMU SACSAA research group. The flyers were also posted on several general noticeboards located on NMMU campuses.

No other measures were taken to advertise the competition, and no researcher or official campaign representative tried actively to raise cybersecurity awareness or attract participation in the competition. Teachers at schools were, however, asked in the invitation letter to support and encourage their students to take part.

Reminders about the competition due date were sent out via the NMMU communique (general notice via email) system to university students. Similar emails were sent to all schools that had been invited to enter the competition.

7.5 Results

Despite large numbers of pamphlets and invitations being sent out, this trial run of the competition elicited only three posters and one video entry.

NMMU students submitted all these entries. Although many schools had expressed interest in taking part, none of those that had been invited to take part submitted any entries.

None of the posters nor the video belonged to any of the cybersecurity topics. All of the entries only featured the topic headers that were depicted on the competition advertisement (Figure 6.4). This resulted in all the entries being generic in appearance and content, and failing to demonstrate any understanding of any of the topics.

None of the entries were considered suitable for use as awareness-raising materials for future audiences. Judging from on the appearance of the posters, it appeared that the target audience had not gained much awareness of any of the cybersecurity or cybersafety issues.

Feedback was requested from schools that had not taken part despite their expressing interest in the competition. Several of the teachers said that they had not felt sufficiently knowledgeable about the cybersecurity and safety subject-domain to assist their students. Some teachers expressed interest in having an expert present material to their students.
7.6 Reflections

Cycle 0’s purpose was to establish a campaign baseline on which future iterations could improve. During this “trial run” several lessons were learnt. These will help to improve future official campaign iterations.

The first lesson learnt was that:

Lesson 1

Timing is important.

Some school teachers gave feedback that the third term was too late in the year to allow them to meaningfully encourage learners to take part. Thus, the researchers realised that to achieve maximum participation it is necessary to take the schedules of the target audience into consideration. Allowing enough time for participants to prepare and submit their entries is important. Based on the results and feedback, it appears that schools are more likely to take part if they are made aware of the campaign early in the year and if teachers can plan for its promotion.

The second lesson learnt was that:

Lesson 2

Advertising and attracting attention to the campaign must be an active, ongoing process

Despite the effort exerted in advertising the campaign competition via post and flyers, participation was extremely low. Feedback showed that invitations and flyers on their own were perceived as impersonal. A more active approach to advertising the competition and convincing schools and learners may be necessary to gain the target audience’s interest and motivate learners and their teachers to take part. The notion that advertising generous prizes was the only incentive required to attract learners’ attention and participation proved false. It was agreed that the prizes were attractive; however, the personal effort required to participate was discouraging.

The third lesson learnt was that in order to:
Lesson 3

Attract school participation and user attention to educate learners, a more engaging education approach was required.

Expecting students to take the initiative to study and research the topics themselves proved unsuccessful. The advertised prizes were intended to give the learners an incentive to learn on their own. These incentives were not enough to motivate the learners to study voluntarily, however. Those entries that were submitted were merely copies of information provided on the campaign advertisements.

The fourth lesson learnt was that it was important to:

Lesson 4

Take into consideration the campaign’s implementation approach and its suitability for the targeted audience.

Cycle 0 took the approach of relying on self-education and evaluation via the competition. For this approach to work, there had to be some level of certainty that the target audience would see the campaign advertising and/or receive encouragement to take part. In practice, introducing and encouraging school learners to take part in a classroom setting offers a greater chance that these learners will be exposed to the campaign; expecting students to notice the advertisement on a noticeboard is less likely to encourage participation. This lesson also contained a sub-lesson: what attracts, and suits one audience may not attract or suit another. Children, young adults, and adults at university will have different worldviews and preferences. In retrospect, the target audience of Cycle 0 was too broad. Thus, sub-lesson 4A was learned:

Sub-Lesson 4A

Target a limited audience with a campaign suited to them.

The fifth lesson learnt was that:
Lesson 5

*The evaluation method for campaign effectiveness should be efficient and simple to implement.*

Cycle 0’s competition called for any poster, or video entries. Most questions received from teachers and potential participants related to the formatting and to the need for tutorials when creating videos for submission. The difficulties involved in making a video may have deterred many potential participants.

### 7.7 Conclusion

Overall, Cycle 0 did not successfully meet its objectives. In relation to C0O1, the competition was not enough to establish a cybersecurity and safety awareness campaign. Based on the results, limited learning occurred. In relation to C0O2, the competition showed its potential as a means of measuring the effect of any educational effort on learners. However, based on the small number of entries and the lack of effective and appropriate education in Cycle 0 it could not be fully explored as an evaluation method.

Although Cycle 0’s campaign and competition were not very successful, a number of lessons were learnt during its implementation and from its results. The lessons from this cycle were considered in the “official” campaign iteration, discussed in the cycles which followed it.
8 Action Research Cycle 1: 2012

Chapter 1

Introduction

Chapter 2

Description of the Context

Information Security and Cybersecurity

Chapter 3

Information Security and Cybersecurity Education

Chapter 4

Methodology

Chapter 5

Development and Detail about the Selected Issues

Theoretical Basis of Action Research Interventions

Chapter 6

Action Research Process

Cycle 0: Pilot

Cycle 1: 2012

Cycle 2: 2013

Cycle 3: 2014

Cycle 4: 2015

Chapter 12

Conclusion
This chapter presents Cycle 1 of the action research process. Cycle 1 examines the interventions conducted on the SACSAA cybersecurity and cybersafety in 2012. This cycle focused on introducing pedagogical principles to the design and implementation of the campaign.

8.1 Introduction

Cycle 1 was the first “official” iteration of SACSAA’s awareness and education campaign. It aimed to improve upon the implementation and effectiveness of Cycle 0’s “trial run”. This was achieved by taking into considerations the lessons learnt from Cycle 0. Cycle 1 was the first in which the researcher was directly involved in the design and presentation of awareness-raising material. The iteration is discussed according to the layout shown in Figure 6.2. This is the second iteration of five action research cycles and campaign years included in the thesis. The following sections describe the design, implementation, and results of the cycle.

8.2 Problem Identification

Cycle 0 established that although many schools were invited to participate in the campaign and competition, none of them opted to take part. Reasons for this lack of participation included:

- timing of the campaign
- impersonal nature of the advertising
- lack of supporting educational materials to help participants and
- the ineffectiveness of a self-driven education approach in this campaign.

Cycle 1 aimed to improve upon its predecessor by addressing some of these issues.

The problems of interest for Cycle 1 were:

- need for a less self-driven education approach and a lack of supportive education material (Section 8.2.1);
- ineffective advertising and lack of participation agreement (Section 8.2.2);
- need for a simplified implementation of the method used to evaluating the campaign's effectiveness (Section 8.2.3).

Each of these problems, and the associated objectives to address the problem, are discussed below:
8.2.1 Establish a more formalised education approach with supporting materials

In order to address the need for a less self-driven education approach with supporting educational materials, C101 aimed at establishing a more formalised education approach.

It is essential that learners are educated about cybersecurity and that the educational material be presented in a manner that is memorable, comprehensive, and suitable for a diverse target audience. Overall, it must be as effective as possible. Accordingly, it is essential that the material be as appealing as possible to as many learners as possible.

One method to improve the probability of an education intervention being effective, is to ensure that the educational effort is as pedagogically sound as possible. Tried and tested pedagogical principles can offer guidance on design, implementation, and presentation of materials. The lack of a pedagogical basis has been identified as a weakness in many existing information security education approaches (Puhakainen, 2006). This is an issue which cybersecurity education efforts should avoid.

In order to address the issue of a more formalised approach with a high probability of being effective for a diverse audience, Cycle 1 – Objective 1 (C1O1) was to: “Establish a more formalized education approach with supporting materials which are pedagogically sound.”

8.2.2 Improve method(s) used to achieve school participation and capture learners’ attention

Cycle 0 involved many campaign advertisements and invitations being sent to schools. This succeeded in attracting participant attention, but did not ensure learner participation (Lesson 4).

In order to educate learners, one must attract and hold their interest. They must be aware of their need for knowledge about cybersecurity issues and practices, and they must want to gain this knowledge. Without an interested and active target audience, the campaign’s efforts would be futile.

Cycle 1 – Objective 2 (C1O2) was therefore to: “Increase school and learner participation, by actively campaigning and advertising the campaign and competition to attract interest and participation”.

181
8.2.3 Simplify the implementation of the method of evaluating the campaign’s effect on learners

It is often difficult to measure the effectiveness of an awareness-raising or training programme. Nonetheless, an evaluation is necessary to ascertain how much information has been retained, the application of cybersecurity concepts and general attitudes toward cybersecurity (NIST 800–12, 2004, pp. 153).

Measuring users’ knowledge after a campaign indicates how the campaign is affecting them. If the users are learning, then it can be regarded as successful. The campaign must be adjusted and improved if learners’ interpretation of concepts deviates significantly from the knowledge base from which the campaign teaches.

Cycle 0’s “trial run” used a competition to gather poster and videos as a method of data collection. The intention was to analyse these posters and videos as part of the qualitative content analysis, which would determine the effect the campaign had on learners.

The competition called for learners to submit posters and videos which they believed could be used to improve other users’ understanding of cybersecurity and safety issues and behaviours. The entries would be their own understanding of the messages they depicted. Conceptually, the evaluation method was sound. However, when implemented it proved challenging when it came to the video entries.

Despite receiving only one video entry, the competition elicited a great deal of communication and questions from several potential participants on how to create, format and submit videos and so on. On the other hand, there were no questions about how to create posters. Therefore, the simpler method of data gathering and encouraging participation was judged more efficient.

Cycle 1 – Objective 3 (C1O3) aimed to address the issue of the overcomplicated method of data gathering and to: “Simplify the implementation of the data collection method used for evaluating the campaign’s effect on learners”.

This section presented the problem identification in Cycle 1 of the action research process. The next section discusses the plan of action for studying and addressing the cycle’s problems.
8.3 Action planning

This section outlines the planned implementation of the 2012 iteration of the SACSAA cybersecurity and safety awareness campaign and competition. Figure 8.1 illustrates this section’s structure.

This section describes how the iteration was intended to be implemented in the cases where schools followed the full (recommended) campaign implementation.

8.3.1 Target audience

Cycle 1 planned to focus on school learners only. The plan was to target learners at primary schools and high school learners in the Nelson Mandela Metropolitan area. The age range of the target audience would therefore range from age 6 to 18. The justification for focusing the campaign on school learners is provided in section 2.6.

Several schools were invited to take part in the campaign during Cycle 1. Of all those invited, three elected to take part in the educational campaign and compete in the poster competition. School A, a primary school, and School AA and School BB, two high schools, opted to take part. The sections below outline the implementation (section 8.4) and the results (section 8.5) of the campaign at these schools.
8.3.2 The Educational Campaign

Following Cycle 1 – Objective 1 (C1O1) the overall education effort was intended to be presented as a more formalised approach, which relied less on self-paced education than Cycle 0. In Cycle 0, the competition was the education motivator, and the means of collecting the data to measure the effect of the “education” on the learners.

In 2012 a decision was made to offer educational material as well as resources. The competition would then be used as a motivation for participation and a method for gathering data on the effect of the educational effort on learners’ knowledge.

This section outlines the planned implementation of the campaign’s educational component. This plan explains the practical implementation decisions and, where applicable, it outlines whether these decisions are pedagogically sound.

To meet C1O1, the first decision made on alterations to the campaign was the selection of a pedagogical approach for that the educational effort would follow. This approach had to be suitable for diverse audiences and have reputable principles that would guide the educational design.

Brain-compatible education pedagogy was selected as the approach for the SACSAA campaign. Section 5.2. provided a theoretical, contextual discussion of brain-compatible education and its principles. Table 8.1 provides a summary of the principles followed in this work.

The remainder of the chapter refers to brain-compatible education (BCE) principles using Table 8.1’s principle numbers, e.g. BCE Principle 1. These numbers are only for reference purposes.

The education campaign needed to appeal to a diverse audience, with different learning styles and knowledge levels in terms of cybersecurity and technology use. The target audience ranges between the ages of 6 and 18. Modern children tend to use technology from a very early age; however, what they use technology for changes and evolves as they get older. For instance, from using technology mainly for entertainment (games, movies etc.), children expand their technological activities to include socialising, browsing or generating content and conducting financial transactions (Oblinger, 2004).

The learners’ topics of interest, and thus the campaign topics and content suitable to the audience, would change as the audience’s needs change. Therefore, the campaign had to provide educational resources which presented and explained the content in a manner that would: appeal
to the various age groups, and to ensure that the material met the educational needs of each age group.

Table 8.1 Brain-compatible principles to be applied

<table>
<thead>
<tr>
<th>Number</th>
<th>Brain-compatible Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A learning experience should be as multifaceted as possible, catering for as many learning styles as possible and providing as many opportunities for each learner to develop as possible (section 5.2.2).</td>
</tr>
<tr>
<td>2</td>
<td>Positive emotions should be used to aid recognition and recall (section 5.2.3).</td>
</tr>
<tr>
<td>3</td>
<td>Relate all new material back to old material and thereby build new knowledge on old knowledge (section 5.2.4).</td>
</tr>
<tr>
<td>4</td>
<td>The search for meaning is innate and occurs through patterning (section 5.2.5).</td>
</tr>
<tr>
<td>5</td>
<td>Every brain simultaneously perceives and creates parts and wholes during the learning process (section 5.2.6).</td>
</tr>
<tr>
<td>6</td>
<td>It is necessary to review material repetitively to solidify recall and recognition (section 5.2.7).</td>
</tr>
<tr>
<td>7</td>
<td>Both the focused and peripheral attention of a learner should be involved in the learning process (section 5.2.8).</td>
</tr>
<tr>
<td>8</td>
<td>Allow learners to progress through the course at their own pace (section 5.2.9).</td>
</tr>
</tbody>
</table>

ISO 27002 recommends that information security education programmes consider and use different forms of education and training, e.g. lectures or self-studies (ISO/IEC 27002, 2013, pp. 13). This includes using various types of awareness-raising materials (NIST 800-50, 2003). BCE principle 1 (as referred to in table 8.1) requires that a learning experience be as multifaceted as possible in order to cater for as many learning styles as possible and to provide many opportunities for learning to take place. Guided by the need for different forms of education recommended by ISO 27002 (2013) and by BCE principle 1, Cycle 1’s education campaign was designed to provide schools and learners with multiple educational resources in multiple formats.

The resources would provide cybersecurity information relevant to the target audience. The materials could be used as given, or incorporated into teachers’ lesson plans or educational activities.

The planned inclusion of multiple resources, some of which discussed the same content differently, would also provide learners with repetitive review material. The repetition would assist
learners in solidifying their ability to recognise, recall and possibly apply the content covered. The inclusion of multiple resources was therefore also an implementation of BCE principle 6.

The planned educational resources included informative awareness-raising materials, and the option of a lecture by a cybersecurity expert. The plan was to expose the learners to the awareness-raising materials and expert lectures, and then encourage them to take part in the poster competition.

The general implementation of the educational effort was planned to be compliant with brain-compatible education BCE principles. In addition, individual awareness-raising materials and lectures were also designed to follow brain-compatible education principles. Each resource is briefly described below.

### 8.3.2.1 Awareness-raising Materials

Multiple types of awareness-raising materials were designed or adopted for inclusion in the campaign (NIST 800-50, 2003). These materials included topic specific flyers, pedagogically designed educational games and reinforcement materials such as a pledge of cyber-secure behaviour and awareness-raising stickers.

The provision of multiple resources and activities takes into consideration BCE principles 1 and 6, allowing multiple opportunities for material messages to be reviewed and reinforced. Some of the materials were more formalised, e.g. topic-specific awareness-raising materials and expert presentations, while others were “fun” educational tools (educational games) or supportive awareness-raising tools (stickers etc.).

Including several types of materials helped in appealing to different learning styles (BCE principle 1) while also attracting the learners’ focused and peripheral attention (BCE principle 7). The more engaged and focused a learner is in the educational experience, the more probable it is that he or she will successfully learn something from the campaign. The included awareness-raising materials are discussed in section 8.3.2.1.1 to section 8.3.2.1.4.

#### 8.3.2.1.1 Topic specific flyers with single security message

The inclusion of flyers or pamphlets is a common method of delivering awareness-raising materials to learners (users) in information security education campaigns. As an awareness-raising tool, they aim to attract the learner’s attention and share a topic-specific message.
Ten topic-specific cybersecurity flyers were adopted from a campaign run by researchers at UNISA. These flyers were selected for distribution as part of the NMMU’s SACSAA awareness-raising and education campaign. They were included because their design and presentation of content was deemed to conform with the recommendations of several BCE principles.

It should be noted that since the flyers were designed by a partner institution, they were not intentionally designed to adhere to BCE principles. However, their design does adhere sufficiently to these principles to be considered BCE principle compliant. Their content was adequate for awareness-raising material; however, more in-depth material would be required to teach learners about the topics they had been made aware of.

The flyers illustrated examples of important cybersecurity and safety issues, a relevant cybersecurity or safety tip or message. Topics included cyberbullying, cyber predators (stranger danger), social networking, password security and several other topics. Figure 8.2 features examples of some of the flyers. The flyers were intended to be used in class and to be posted on noticeboards in school classrooms or corridors.

![Flyers](image)

Figure 8.2 Single topic awareness-raising posters provided as supporting material (source: UNISA campaigns)

The flyers communicated content on single topics to make their message easily identifiable and unambiguous. These were awareness-raising flyers, designed to be visually attractive (aesthetically appealing) and to discourage distraction (BCE principle 7).
The designs made use of colour, text, and images to attract learners’ attention and to convey their message (BCE principle 1, 2 and 7). Text and images worked together to convey the message on each flyer.

The text explains the message and, in some cases, provides tips on how to secure oneself against the particular cyber threat. Figure 8.2 shows an example of the textual tips on the first social networking poster. The images depict realistic or analogous images which further emphasise the cybersecurity threat. The explanations and images typically relate the message to similar known concepts (BCE principle 3 and BCE principle 4). In so doing this, the flyer’s message builds upon the learner’s presumed existing knowledge. Therefore, it contributes to the learner’s understanding of the concept by associating the messages as part of a “pattern”. Examples of flyers and how they implemented this briefly described below.

In Figure 8.2, the cyber predator flyer expresses the concept of protecting oneself against cyber predators in the message of shielding one’s self against an actual predator (or stranger). The flyer emphasises the danger and need for protection. Similarly, the third poster in Figure 8.2 relates the concept of cyberbullying to real-world bullying. By depicting a real fist coming through the computer screen and a child crying or hiding it emphasises that the two actions are related, hurtful and can cause fear or sadness. Strong images and explanations such as in these examples encourage learners to identify with the message (BCE principle 2).

Colour was also used to influence the emotional state and gain the focus of learners (BCE principle 2 and BCE principle 7). Colour has the potential to increase the probability of environmental stimuli being encoded, stored, and retrieved successfully. The choice of colours and their manipulative aspects can, however, influence the extent to which they influence human attention, retention and memory performance (Olurinola & Tayo, 2015).

The background colours of the posters were yellow, blue, red, or green. Yellow arouses positive feelings and was aimed at attracting learners’ attention (Taylor, 2007; Walker, 1999). A positive mood can enhance a learner’s attentiveness (BCE principle 7). Green encourages productivity, concentration, clarity and long-term energy (Taylor, 2007). Red can be engaging and emotive but should be used sparingly. Both blue and green can be calming, and assist in concentration (Walker, 1999).

The aim of the flyer designs was to attract learner’s attention, communicate the content, illustrate the concepts, to increase understanding as much as possible and to make the posters relevant
to learners. The flyers were designed to appeal to all learners; however, they were most attractive to learners with a visual learning style (BCE principle 1).

The flyers were intended for use as supplementary material in lessons or discussions led by teachers or peer groups. They were intended for display on noticeboards in classrooms or other places where learners could read them. Displaying these flyers at all times meant that if a learner lost focus during lessons or other activities, the flyers could potentially attract their attention again. In this way they might also learn from the flyers. This appeals to BCE principle 7, which states that learning can to some extent take place even when the material appeals only to the learner’s peripheral attention. Images are particularly useful in this regard as a glance at them can develop some understanding of the flyer’s message.

**8.3.2.1.2 Snakes and Ladders game**

Several versions of a pedagogically designed educational game was planned for inclusion in Cycle 1’s awareness-raising material resources. These games represent an informal education tool for educating learners about cybersecurity topics. This section describes the game that was selected, redesigned, and planned for distribution and use as part of the campaign.

This campaign targets school learners. The current generation often perceives learning as a “boring” activity because existing teaching methods are incompatible with how they learn (Tang & Hanneghan, 2011). Therefore, using traditional approaches only to teach cybersecurity may not always be suitable for this young target audience.

Education studies have found that school children show an interest in using games for learning purposes (Roslina & Jaafar, 2009). Gameplay educational approaches build on natural learning methods used by the young of any species to gather important life-skills. Previous work has shown that education that is fun is an effective mechanism for children as it engages their interest and discourages them from disassociating from what is being learnt (Reid, Van Niekerk & Von Solms, 2011). Not all games are necessarily educational, however. Grounding a game in a proven pedagogy increases its potential as an effective education tool.

Adding an educational game to the campaign resources was worth investigating. This required the creation or redesign of a game to ensure that it would comply with brain-compatible pedagogical principles. The game targeted an audience of learners between the ages of 5 and 18 and had to be suitable for the whole target audience. Thus a “family-friendly” style of game was needed. While selecting and redesigning such a game, the following characteristics were
considered: age-appropriateness, content, user-friendliness, learnability, and its potential to fit in with brain-compatible education principles.

Existing children’s games that where suitable for a broad age group were considered as the basis for the game’s design. “Snakes and Ladders”, a popular board game played by children worldwide, was chosen to be the cybersecurity educational game’s foundation for the following reasons:

1. Having existed since the 2nd century in India, it is a popular game, the rules of which are familiar to the target audience (Avedon, 2010);
2. Its original purpose of teaching children the difference between "good and evil" is similar to teaching children good and bad cybersecurity lessons (Avedon, 2010);
3. Thirdly, it now targets children from age 5+. Primary school children regularly play it; however, it can be played by individuals of all ages.
4. Pedagogical principles and appropriate cybersecurity educational content could be easily incorporated into the design.

The design, content, and game play rules of the redeveloped game are discussed below.

8.3.2.1.2.1 Design

“Snakes and Ladders” was selected as a good redevelopment candidate as brain-compatible pedagogical (BCE) principles could easily be applied to its design and implementation (Figure 8.3). This section briefly describes some applications of BCE principles.

Firstly, the game had to cater for learners with different learning rates. Brain-compatible education advocates self-paced progression (BCE Principle 8). The game achieved this via the turn-based play, which requires the player to throw dice and move a token, and read a lesson. This allowed the learners to play and learn at their own pace, while encouraging progression.

Secondly, the game’s design had to be interactive and “fun”. This was necessary to provide a social and communicative, peer-supported learning experience. This was considered essential as it implements BCE principle 1 by appealing to multiple learning styles, especially those favoured by kinaesthetic and auditory (social) learners. Additionally, these characteristics capture and maintain learners’ interest/focus while positively stimulating their emotions (BCE principle 7 and BCE principle 2).
Figure 8:3 Snakes and Ladders password security themed board game

The “fun factor” of the game appeals particularly to the learner’s positive emotions (BCE principle 2). This allows a learner to better focus, learn, and retain learnt content. Aspects of the game’s design appealing to this BCE principle include: its inherent entertaining, interactive, and socially competitive nature; and its reinforcement mechanisms that encourage changes in emotional state (e.g. happiness when ascending a ladder). The incentive of winning also increases the entertainment factor and appeals to BCE principle 2 while encouraging progression through the game (BCE principle 8).

The colours used on the board were also intended to influence the state of the learner’s emotions and focused on implementing BCE principle 2 and BCE principle 7. The background of the board’s squares was coloured various shades of yellow and green. Yellow elicits positive moods and attracts the learner’s attention, while green encourages productivity and long-term energy (Taylor, 2007). The design also fulfilled BCE principle 1 by engaging visual learners.

The final design considerations relate to educational reinforcement mechanisms. The educational game needed to provide consequences for lessons learnt during the game. This was easily
introduced into “Snakes and Ladders” as its original purpose was to teach the difference between good and evil using such mechanisms.

The snakes and ladders were placed randomly on the board, alongside information security lessons (Figure 8.3). Positive lessons (below ladders) provided reinforcement by allowing ascension of the ladders. Conversely, negative lessons (above snakes) were reinforced by forcing the player to descend the board via the snakes. This design associated negative consequences with negative messages and positive consequences with positive messages. This facilitated behaviour and knowledge patterning of multiple concepts (BCE principle 4 and BCE principle 5).

8.3.2.1.2.2 Content

Several games were created for various topics, including social networking, password security, and virus security. Each of the boards had a similar design, but different content. The board depicted in figure 8.3 contained secure password management content. Various rules specifying the Do’s and Don’ts of password security were placed above snakes and below ladders (Figure 8.3). These lessons are listed in Table 8:2.

Table 8:2 Password lessons of Do’s and Don’ts

<table>
<thead>
<tr>
<th>Do’s</th>
<th>Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td>You gave your password to your parent or guardian.</td>
<td>You gave your password to a friend.</td>
</tr>
<tr>
<td>Your password is at least 8 characters long.</td>
<td>Your password is less than 5 characters.</td>
</tr>
<tr>
<td>You change your password at least once a month</td>
<td>You wrote your password down.</td>
</tr>
<tr>
<td>Your password is not a word in the dictionary.</td>
<td>You used your name or your pets name as a password.</td>
</tr>
<tr>
<td>You used characters like !,#,$ in your password.</td>
<td>You used the same password everywhere.</td>
</tr>
<tr>
<td></td>
<td>Your password is easy to guess.</td>
</tr>
</tbody>
</table>

The lessons were written as if the player had, or had not, complied with a rule of secure password management. This “learner-centric” perspective serves to implement BCE principle 3 of brain compatible pedagogy. The lessons built on scenarios that a learner may have been familiar with personally or via observation; in this way, new knowledge was related to older knowledge. The lessons were learned while following the rules of the game.
8.3.2.1.2.3 Rules

“Snakes and Ladders” can be played by two to six players. In sequential order and starting from “Start”, each player rolls the dice and moves his or her token along the board’s sequential squares according to the number thrown. If the square a player lands on contains an information security educational message, he or she reads it aloud and performs the required action. The verbal sharing of the message helps the learners to consider the lesson cognitively (BCE principle 1).

If the message is a “do not” lesson, the player is swallowed by the snake and moves the token to the square containing the snake’s tail. If it is a “do” lesson, the player ascends the square’s ladder and places his or her token in the square at the top of the ladder. The first player to reach the 50th square (Finish) is the winner.

The effectiveness of this game as a cybersecurity educational tool was assessed by means of a case study. Section 8.3.4.6 discusses the research instrument.

8.3.2.1.3 Cybersafety pledge

A personal pledge form was included as part of the awareness-raising materials (Figure 8.4). Designed by one of the SACSAA alliance research groups, the pledge form was intended to make the campaign lessons more memorable for the learners.

The pledge was a commitment the learners made to their own personal internet-safety. The assumption was that, once it was formally made, the bind between the promise(s) and future action would be strengthened and more likely to result in the desired behaviour (Katzev & Wang, 1994). The pledge includes promises to:

1. Never disclose their personal information over the internet;
2. Be aware that people can misrepresent themselves on the internet; and
3. Inform their parents or guardians if an online stranger requests their personal information.

The pledge form was to be signed by both parents or by an alternative caregiver. The teachers involved in distributing the awareness-raising materials and the experts involved in the education campaign encouraged learners to make a cybersafety pledge to themselves and Cyber Sid (a SACSAA partner’s campaign mascot).
The pledge reinforced specific messages that were communicated by other awareness-raising materials (BCE principle 6). The pledge would appeal to all learning styles; the written pledge appealed to visual learners, while the act of taking the pledge (by reciting or hearing it) appealed to auditory and tactile-kinaesthetic learners (BCE principle 1).

8.3.2.1.4 Cybersafety 101 flyer

The cybersafety 101 flyer was designed and printed after the first invitations to participate had been sent out. The flyer listed seven basic cybersafety “rules” that learners could follow to help them stay safe online (Figure 8.5). The “golden rules” were each listed with a brief explanation. This type of awareness-raising material will appeal particularly to learners with a visual learning style (BCE principle 1).

The contents of this flyer contained messages which were also communicated by the single topic flyers, and which formed the basis of the cybersafety talks presented at schools by researchers. The flyer content provided both an “overview of these messages” and the opportunity to review the messages repetitively when used in conjunction with the other awareness-raising materials and resources.
The overview “summary” component of the rules was used with other materials as an implementation of BCE principle 5. It provides the individual “topics” and messages to which other materials’ messages can be related. Because the flyer can also be used to review material it fits in with BCE principle 6 by enabling repetitive review of concepts. Finally, depending on when the flyer is introduced to learners in relation to the other awareness-raising materials, the messages they carry can build upon messages and knowledge to which learners have previously been exposed (BCE principle 3).

**8.3.2.2 Expert presentations**

Lectures and training sessions are a frequent and popular technique for delivering material to an audience in most awareness-raising, training and education programmes (NIST 800–50, 2003). Schools were given the choice of having a cybersecurity expert from the SACSAA NMMU.
research group visit them to deliver an educational presentation to learners. It was not compulsory for schools to host these talks; however, it was the recommended plan of action.

Schools could request that experts visit them. The request could be made:

- during the first meetings with the SACSAA representative,
- via the request form included in the invitation packages, or
- via the SACSAA website.

Presentation sessions at schools could be scheduled for any time during the campaign period.

The planned 2012 presentation title was “Cybersecurity Self-defence”. The content of the talk and its supporting materials were designed to be presented in a sequential manner. It began by outlining the talk’s objectives. Then it explained why cybersecurity is necessary. A description of various cybersecurity threats, their effects, and the controls needed to protect against them was then provided. All the explanations gave both a societal and an individual (learner) perspective of the discussed issues and solutions. The key message within the talk centred around what were dubbed “the seven rules of cyber self-defence”, namely:

1. Protect your own computer
2. Have a good password
3. Keep your PRIVATES private
4. Don’t trust people you meet online.
5. Stay legal!
6. Don’t be a bully!
7. Trust someone.

Each of the rules described cyber secure behaviour. Examples of the related cybersecurity issues and potential solutions were given to justify each rule of behaviour and explain how to implement it. Examples and explanations could be realistic, analogous, and/or contextualised.

The examples illustrated the concepts in contexts that the learners were familiar with. Some of the graphics and narratives used humour to gain attention, elicit emotion and ease tension after tough topics. These examples were intended to make it easier for the learners to relate to the material on a personal and emotional level (BCE principle 2 and BCE principle 4). Finally, practical tips and advice were also included with each rule to guide the learners in their practical application of the cybersecurity rules and behaviours.
Where applicable, cybersecurity topics were explained by relating them to non-cyber counterparts or concepts. Examples of this explanation format included explaining:

- cyberbullying in relation to bullying,
- stranger danger online to stranger danger in the real world,
- how physical security is compared to locking up one’s home or shielding oneself against an attack; password security is related to access control into secret hideouts, bank accounts and safes.

These explanations assist in relating new knowledge to existing knowledge (BCE principle 3) and forming a conceptually patterned understanding of the issues (BCE principle 4).

All the content in the presentation related to the content explained in the other awareness-raising materials given to schools. However, the presentation was more educational, as it offered a more in-depth explanation. It also aimed to help learners derive a more conceptual and practical understanding of the cybersecurity issues and behaviours. The expert presentation provided an opportunity for learners to review material (BCE principle 6) if they had been exposed to the other awareness-raising materials. In other cases, it taught them basic knowledge and other materials offered revision opportunities.

The sequential presentation of the material, and the perspective of the explanations aids in explaining cybersecurity issues both as individual concepts and as related concepts (BCE principle 5). It also ensures that learners are introduced to the concepts in a logical order and that they have the prerequisite knowledge for learning each concept (BCE principle 3).

Each topic builds its knowledge upon the knowledge taught by other topics. An example of this is: learners should be introduced to the concept of not sharing their personal information before the concept is expanded upon by the need to be aware of the dangers of social networking and strangers trying to obtain their personal information. The inclusion of multiple formats of explanations and examples also assist implementing BCE principle 5 and other BCE principles.

In accordance with BCE principle 1, the presentation was designed to be as multifaceted as possible in order to appeal to multiple learning styles. The first design decision was to use a Prezi presentation format as the talk’s supportive material. Prezi is a visual storytelling software alternative to traditional slide-based presentation formats. It is designed to create more engaging, persuasive and memorable presentations than alternative boxed-in slides (Prezi, 2016).
Prezi presentations feature a map-like, high-level view of the talk. The users can pan between topics at will, zoom in on desired details, and pull back to reveal context. This feature enables the materials to flow with the presentation dialogue much like a conversation (Prezi, 2016). The purpose of this style of presentation is it is to:

- visually engage the audience (BCE principle 1),
- attract the audience’s attention and maintain their focus while explaining the content (BCE principle 7); and
- provide a visual cue to help learners “slot-in” the newly learnt concepts into conceptual, global “slots” that were briefly described in the presentation’s overview and the outlining of the objectives (BCE principle 5).

The second design decision related to BCE principle 1 was the inclusion of multiple explanation formats. Various explanation formats were used for the contextual explanations, as well as for explaining the rules of cyber self-defence. To differing degrees, the explanations included: on-slide text, images (photographs or other illustrations) of the concepts or controls, and/or infographics where applicable. A few, select videos were also included as an initial explanation of why cybersecurity is necessary. The use of images with the textual and verbal explanations was intended to help learners build strong verbal-visual associations between the concepts and the illustrated examples, thereby making what was taught more memorable (BCE principle 5).

All the presentation and explanation formats were meant to attract the learners’ attention and focus it on the presented topic(s) (BCE principle 7). The learning process should engage learners; other attempts to engage the learner included interaction between the expert and the audience.

During the presentation, interaction with the audience was encouraged. The possibility of interaction with the audience is one of the reasons lecturing is a beneficial training technique (NIST 800–50, 2003). These interactions involve the expert requiring input (showing of hands, volunteering of ideas or answers) from the audience, and occasionally from individuals. Examples of input could include learners raising their hands if an example applied to them; or voting if they thought a cybersecurity statement was true or false. Opportunities for interaction could be both planned and improvised.

An additional form of interaction that was included was a question and answer (Q&A) discussion period at the end of the presentation. Learners could ask the expert any question they had which was relevant to cybersecurity topics. These interactions, accompanied by the expert’s consistent spoken explanations, were intended to appeal to, learners with auditory and kinaesthetic-tactile
learning-style preferences (BCE principle 1). The question and answer session interactions were also opportunities for the expert to give formative feedback to the learners (BCE principle 2). This feedback would in turn encourage reflective thought in learners (BCE principle 4).

During all the interactions, rewards in the form of cyber awareness stickers (Figure 8.8) were given to learners who actively took part. Receiving a reward was planned to elicit positive emotions which learners would associate with the campaign and the learning experience.

The expert led a verbal swearing of the Cybersafety Pledge after the question and answer part of the presentation. This served as the final reinforcement of the concepts presented and the campaign’s intention of making the material interesting and relevant to the learner (BCE principle 2 and BCE principle 6). The pledge concluded the presentation.

Overall, the presentation included frequent references to topics, multiple examples, and explanations of the concepts, and used several media formats and activities to present the content. Thus, the entire talk was a broad implementation of BCE principle 6.

### 8.3.2.3 Branding

As part of the actions taken in meeting C1O2 and based on expert advice from NMMU marketing personnel on including branding, a design decision was made to include branding symbols in the campaign and its materials. Two types of branding would be included: the SACSAA logo (Figure 8.6) and a campaign mascot (Figure 8.7). The SACSAA logo (Figure 8.6) was included on all the campaign’s educational resources.

![SACSAA logo included in campaign material](image)

A research partner in the SACSAA alliance developed a mascot for use in the awareness-raising materials. This mascot is a blue and green robot figure with a padlock on its chest (Figure 8.7). The mascot was named “Cyber Sid”. The pledge form and other awareness-raising material distributed as part of the larger national campaign was branded with the mascot. For the sake of convenience and coincidentally compliance with BCE principles in its design, Cyber Sid was the mascot included in NMMU’s SACSAA educational material.
The inclusion of a mascot is an established technique for delivering awareness-raising material (NIST 800–50, 2003). It is a technique which lends itself to dissemination of multiple messages. Macklin (1996), on the learning of brands from visual cues, it was concluded that using two visual cues (figures or colours), improves the memorisation of brand names and symbols. The mascot can be included on various awareness-raising, training, and educational materials. Its consistent use can act as a unifying “brand” for the educational effort. A mascot helps keep a constant presence within the campaign. Experts and campaign representatives could change over time; however, the mascot will be a consistent advocate for the message.

The presence of the mascot was planned for the following purposes:

- to appeal to visual learners (BCE principle 1);
- to establish strong visual-verbal (word-picture) associations between the mascot and the campaign’s cybersecurity or cybersafety messages (BCE principle 5);
- to aid in unifying the awareness-raising and educational materials and resources as a collective campaign effort (BCE principle 5). Learners will subconsciously learn this association if the mascot attracts their focused or peripheral attention (BCE principle 7);
- to make the material more relatable the mascot could be included as a “friend” or “hero” for the learner in relation to the cause. The mascot could become a character the learners trust and/or like. Positive feelings towards the mascot could transfer to the campaign and the cybersecurity or cybersafety messages which the mascot supports (BCE principle 2).

Overall, the mascot was intended to make the material more relatable and recognisable. Whether the mascot was successful in making an impact on learners was an issue of interest for Cycle 1.
8.3.2.3.1 Cyber Awareness Stickers

A large collection of stickers was designed by researchers at UNISA and used in the campaign. The cybersecurity awareness stickers (Figure 8.8) were branded with Cyber Sid (Figure 8.7) the words “Be cyber safe” and the Alliance’s website address.

Figure 8.8 Cyber Sid Cyber Awareness Sticker

The stickers were also used as a reward programme. This is a common technique in delivering awareness-raising material (NIST 800-50, 2003). The intent was to reward learners who actively took part in the expert presentations. Learners who asked questions, answered questions, or helped in other ways during the presentation were all given stickers. Learners who received the stickers, could also wear them, or display them somewhere, reminding everyone who saw them about the cybersecurity campaign and its messages.

8.3.2.4 Invitation to participate

Cycle 1’s plan, based on lessons learnt from Cycle 0, was to begin the campaign earlier in the year. This was intended to improve the likelihood of schools allowing their learners to take part in the competition. The earlier start date and the unchanged end date allowed an extended time-period for teachers to encourage participation and for learners to create posters. Cycle 0’s feedback indicated that teachers needed more time to encourage students to participate, and to plan for lessons to provide learners with time to work on the poster or learn about the topic. The due date for the competition entries remained the last week of October (SACSAA Cybersecurity and Safety awareness week).
The plan to advertise and encourage participation built on what was learnt in Cycle 0. Initially, invitations and information packs were sent to schools in the metropole via post. The packs contained:

- a professionally designed advertisement (Appendix D Figure 2)
- some awareness materials (topic specific awareness flyers (Figure 8.2), cybersafety pledge forms (Figure 8.4))
- a request form (and contact details) for a free expert presentation, and
- a cover letter explaining the importance of cybersecurity, the campaign and why it was relevant to children.

Additional plans were made to visit schools in person to talk to the principal or teachers who would be involved in championing the campaign at the school. This decision aligned with BCE principle 2 and BCE principle 5. The visit would involve human interaction and the establishment of “trust” in the campaign. It also served as an opportunity to explain the campaign’s importance as a part of a whole. Its importance would be explained in relation to: learners, the school itself, and the larger SACSAA campaign in relation to the establishment of a societal cybersecurity culture.

During their visits to schools, the researchers intended to deliver additional material in the form of a flyer providing a summary of important cybersafety rules (Figure 8.5) and a cybersecurity “Snakes and Ladders” game (Figure 8.3).

The purpose of the cybersecurity poster competition was explained from an educational and research perspective both in the participation packs and during the visits. Schools were allowed to participate in the educational component of the campaign but to opt out of participating in the competition.

### 8.3.3 The Competition

Invitations to take part in the poster competition were included in the educational campaign’s information and resource invitation packages.

Overall, the purpose of the competition did not change from that of Cycle 0. Firstly, the competition contributed to the educational part of the campaign. Secondly, the competition was the primary method of gathering data on participating learners’ knowledge levels. Nevertheless, the implementation of the competition differed in the following ways:
• **What to enter**

Cycle 0 found that the majority of queries from prospective participants related to technical questions on how to create and submit videos. These queries were not the focus of the competition: the content was the priority. C1O3 aimed to simplify the method of evaluating the campaign's data gathering method.

The plan for Cycle 1’s competition was therefore to make the competition more focused and streamlined. A call was made for *poster* entries only for the competition. Cycle 1’s video category was removed. Learners could submit only one poster, depicting one or more cybersecurity and/or safety topic.

• **Prizes**

As in Cycle 0, generous prizes were advertised to motivate learners to take part. However, this year there were no cash prizes. Prizes were offered for:

a. the “Top 13” entrants (generous electronic device prizes)
b. The school that provided the most participants (a projector)

Winning posters from the competition would be incorporated into future SACSAA campaign awareness-raising materials. This served as an additional incentive for the participants to take part. Use of the learner’s poster was meant to add prestige to the act of winning and taking part in the campaign. It also served as an educational resource for future campaigns. Re-use of the children’s posters in future campaigns was also a partial implementation of BCE principle 8, in that it allowed some learners to “see their successes” and acted as a “learner’s log”.

Overall, the competition was also an implementation of the recommendations of BCE principle 8. Learners were still to be encouraged to pursue additional self-paced study in the areas cybersecurity which interested them. This was in addition to classroom exposure to the cybersecurity awareness-raising materials, and attendance of the expert presentation (if allowed at the school). The competition allowed learners to learn about cybersecurity at their own pace, and then required them to show what they had learnt through the creation of posters. The competition would allow the learners sufficient time to complete the learning process and the accompanying poster. However, ultimately there would be a final submission date for the poster and by extension a completion date for the learning process.

The competition was also an implementation of BCE principles 2, 3, 4, 6 and 7. In creating the posters, learners were given the opportunity to: reflect on and review what they had learnt (BCE
principle 6 and BCE principle 7) and to relate conceptually and emotionally what they have learnt to their own context, understanding or first-hand experiences (BCE principles 2, 3, 4 and 7). Engaging learners’ logical and creative thought processes helped to engage both their focused and peripheral attention (BCE principle 7).

8.3.4 Measurements for use in the analysis of the campaign

The success of the campaign was to again be evaluated using the data gathered from the poster competition. All poster entries were included in a qualitative content analysis. The analyses were conducted as described by Krippendorff (2004). In this analysis, the following questions were asked in assessing each poster:

1. How many learners took part? (section 8.3.4.1)
2. What topic(s) is covered by the message(s) in the poster? (section 8.3.4.2)
3. Is the poster specific to one category (form factor) of device? (section 8.3.4.3)
4. How well has the cybersafety message been internalised (in the researcher’s opinion)? (section 8.3.4.4)

These four questions and their related measurements were used to analyse the effectiveness of the cybersecurity and safety education campaign. A separate analysis in the Cycle 1 campaign involved the measurement of the effectiveness of a cybersecurity educational game, which was designed to be pedagogically sound. This game was part of the educational aspect of the campaign. The question asked in relation to this analysis was:

5. Was the robot mascot (Cyber Sid) or other branding present in the posters? (section 8.3.4.5)

These questions are briefly elaborated upon below. Reasons for the measurements are provided, and methods for gathering the measurements are outlined.

8.3.4.1 Learner participation

The number of participants was expected to vary from school to school. Participation was completely voluntary. However, trends in the number of participants from a school over time, or in comparison to other schools, could correlate with changes or differences in the campaign’s real-world implementation each year and in each school. Learners were allowed to submit a single
poster; however, this poster could depict multiple topics. Therefore, the number of posters submitted would indicate the number of learners taking part.

### 8.3.4.2 Posters per topic

The first question had multiple purposes. Firstly, it aimed to determine how well the messages contained in the “Cybersafety 101” flyer and the expert presentations had been received by learners. Secondly, it was used to determine which specific topic(s) the learners considered particularly important. Thirdly, it was used to measure whether there was a difference between those topics considered important by primary school children and by high school children.

As part of the competition rules, a single poster could reflect an unlimited number of topics, so the analysis of the posters was expected to reflect this in its tallies. The analysis examined the images and text to determine the topics that had been depicted or described. It was expected that topics would relate to the themes and topics covered in the cybersecurity resources, e.g. the Cybersecurity 101 flyer and the expert presentation. As the analysis was conducted, topics were identified and grouped within the results.

### 8.3.4.3 Posters per Category of Device

This question aimed to determine whether learners associated the campaign’s cybersecurity or cybersafety messages with a more traditional computer, or with a mobile device, or if they made no distinction between the two. If they differentiated between them then more effort would have to be made to encourage learners to apply their knowledge to the context for which it was intended. If the poster depicted or mentioned only a specific device in relation to the cybersecurity or cybersafety.

The first potential category was that of “computer”. This category would refer to more traditional computers such as desktop computers or laptops. The second category was “mobile device”. This category included cell phones, tablets, portable game systems and other portable devices. The final category was for posters with no specific device association.

### 8.3.4.4 Internalisation of Cybersecurity or Cybersafety Message

Internalisation refers to learning which affects knowledge, attitudes, and behaviour (KAB). An analysis of the posters and the messages/scenarios they depict shows how informative lessons
were perceived and the degree to which they had been internalised. This question attempted to assess how well the child had internalised the message(s) illustrated in the posters. A poster was subjectively categorised according to one of four levels of internalisation:

- **“As given”**
  This category was assigned if a poster repeated a message from the flyer more or less verbatim.

- **“Rephrased in own terms”**
  This category was assigned if the message was expressed in the child’s own terms and showed some interpretation.

- **“Fully internalised”**
  This category was assigned if there was clear evidence that the child also understood the implications and/or consequences of not adhering to the message’s advice.

- **“Un-internalised”**
  This category was assigned if the poster showed no internalisation or the poster could not be interpreted by the researcher, i.e. was not comprehensible or related to a cyber platform, issue, or scenario.

It is possible that raised awareness levels (indicated by internalisation) and any resulting behaviour modifications could contribute to the fostering of a cybersafety aware culture amongst these participants. Examples of posters in each category are provided below. The first example is a fully internalised poster (Figure 8.9).

This poster depicts a message to avoid bullying. The image on the poster illustrates how the learner interpreted the concept of cyberbullying:

*A character called Sam sent an untrue message to other children claiming, “Jo said she likes Mike”. Jo is crying because she never said this. Mike is confused because he was unaware that Jo liked (had a crush on) him.*

This suggests that the child understood that false messages about others could be interpreted as cyberbullying. The learner also understood that such an action could hurt others, hence Jo’s tears. By showing the same message on all the depicted characters’ devices the creator of the poster indicates that she understands that such bullying often occurs in a public forum and is not limited to one-on-one communication. The text of the poster (“Never send untrue messages”) confirms that this is a situation that she wishes to warn others about.
The second example is a poster which was categorised as an internalised message in that it had been “Rephrased in own terms” by the learner (shown in Figure 8.10). The poster shows the campaign mascot expressing important cybersafety and security tips. These messages relate closely to the messages cited in campaign materials and presentations. Examples of these tips and messages are:

- “Don’t trust anyone you meet on the internet”: this is a paraphrase of the cybersafety 101 pamphlet’s (and expert’s talk) message “Don’t trust anyone online”. It contextualises this message and indicates that the student understood online to mean “on the internet”.
- “Don’t forward nasty things to people (Cyberbully)”: this is a paraphrase of the cybersafety 101 pamphlet’s (and expert’s talk) message “Don’t be a bully”.
- The depiction of crossed out personal details on a computer screen relates to the cybersafety 101 pamphlet’s (and expert’s talk) message “Never share personal details online”. The poster also provides examples of the types of information one should not share.

The learner has rephrased the messages or depicted them graphically. The poster contextualises some of the messages, and provides examples. This means that more
internalisation has occurred than would have if the learner had illustrated exactly what was said in the materials or by the experts. However, no depiction or explanation of why these messages matter, e.g. what the consequences of not following the tips, was included.

Figure 8:10 Example of a poster with message “Rephrased in own terms”

The third example is a poster which was categorised as depicting a message internalised only “As given” by the educational material or expert presentations (Figure 8.11).

The phrasing of these messages was similar to what was used when teaching the learners. However, it the poster does not include examples or explanations of the messages, which would have indicated more in-depth understanding. The learner accepted the message as it was presented but has not attempted to relate it more closely to the material and its messages.
The fourth and final example is a poster that was not internalised (Figure 8.12).  

This poster attempts to address the topics of viruses or malware, and the dangers posed by strangers online. However, the illustration and text do not make the messages clear, nor are the messages related specifically to cybersecurity as no technology or online symbol is depicted.
8.3.4.5 Presence of mascot or logo

The purpose of the brand is to create a brand identity for the campaign, which could be a good advertisement and aid in building a rapport with learners in the target audience. The purpose of this question was, firstly, to determine whether students had noticed the mascot and/or logo and, secondly, to determine whether learners associated the mascot and/or logo with the campaign messages. Overall, the answers to these questions would assist in determining whether mascots contribute to building a brand identity for the SACSAA campaign.

8.3.4.6 Evaluation of pedagogically sound cybersecurity education game

The use of educational games and with a strong pedagogic foundation are recommendations made in information security education literature (Ariyapperuma & Minhas, 2005; Bishop & Frincke, 2005; Fung, Ieee, Khera, Ieee, & Depickere, 2010; E. C. Johnson, 2006; Puhakainen, 2006). However, the use of a pedagogically designed game to educate school learners about cybersecurity is seldom reported upon. During the implementation of this aspect of the study, “Snakes and Ladders” was specifically redesigned to comply with the principles of brain-compatible education (BCE) and to teach cybersecurity concepts. The researchers wished to evaluate the effect of the game, if any, on learners’ cybersafety knowledge levels.

In order measure the immediate and the long-term effects of the game on learners’ knowledge levels, a case study was required. The evaluation portion of the research followed procedures from case study protocols described by Yin (2009).

The research artefact, password security “Snakes and Ladders”, is described in Section 8.3.2.1.2. This section describes the data and the two-part research instrument used to gather the required data. The research instrument is included in Appendix E. The first part targeted learners, while the second part targeted teachers.

Part one of the research instrument consisted of a set of informal assessments that could be used by teachers to measure whether learners had gained knowledge about secure password management by playing the game. The assessments were in a quiz format (survey-like) consisting of close-ended, multiple-choice questions relating to a few selected lessons that had been included on the board. These questions assessed whether learners had learnt these lessons. The design of the informal assessments is discussed in depth in Appendix E.
Part two of the research instrument consisted of a few interview questions targeted at teachers who allowed their classes to play the game. The interview questions were designed to elicit the teacher’s perceptions of the effectiveness of the game as a teaching tool and its perceived effect on learners’ knowledge and behaviour.

Both parts of this research instrument were implemented together with the research artefact in the case study. The implementation of the case study is described in section 8.4.1.1. The results of the case study are presented in section 8.5.1.6.

Section 8.3 outlined the recommended implementation of this campaign iteration for Cycle 1. The next section will describe the actual implementation of the campaign iteration.

8.4 Implementation

As recommended, the campaign was to be implemented exactly as outlined in section 8.3 above. However, the real world is rarely ideal or predictable. Participation in this campaign and competition is entirely voluntary for learners and schools. Schools can also make several decisions that can influence the campaign’s implementation. These decisions include whether to allow:

- participation by the school’s learners
- communication between the campaign representative and the principal or the teachers involved
- guest talks at the schools by subject experts
- use of the provided supporting material in or out of the classroom
- active encouragement of learner participation by the teachers, or passive advertising using a noticeboard
- participation of teachers or learners in additional research activities.

This section describes how the campaign was implemented at each school which chose to take part and did submit posters.

As planned, the campaign began earlier in the year. The invitations were sent via post to many schools in the Nelson Mandela Metropolitan Area. In addition, and to attract more participants, the researcher visited many schools in person to advertise the campaign and explain its purpose to teachers and learners. The teachers were asked to encourage learners’ participation in the campaign and competition. Specific use of the educational resources was not prescribed;
however, as a minimum requirement, teachers were asked to display the resources on noticeboards or in classrooms. Inclusion of the material in relevant or dedicated classes was, however, the recommended use of the resources.

Media coverage of the campaign was provided in local newspapers and on air on radio stations. This coverage led to several school outside of the original invitation pool requesting competition information, invitation, and participation packages.

Of the invited schools, only three chose to take part in the educational campaign and the competition. These schools were visited in person by the researcher during the invitation phase of the campaign. One primary school (School A) and two high schools (School AA and School BB) took part (Table 6:1). The campaign’s implementations at each school are briefly described below.

8.4.1 School A

School A was the first primary school, and the third school, in the invitational phase that the researcher invited in person to take part in the campaign and competition. The researcher had a meeting with the school principal and the life-orientation teacher. The researcher explained the importance and relevancy of the campaign, and provided the school with the educational resource package.

The resource package included: the letter of invitation, the topic-specific flyers, each with single security message, the “Snakes and Ladders” games, the cybersafety pledge, cybersafety 101 flyer, competition advertisement poster and a form to request an expert presentation at the school. This was also the first school to request an expert presentation.

8.4.1.1 Evaluation of pedagogically sound cybersecurity education game

Teachers from School A helped to measure the effectiveness of the pedagogically designed game in teaching learners about specific topics. School A provided access to information on a grade 5 class’s use of the game. The class consisted of 11 students between the ages of 11 and 12. They used the password security version of the game. A case study was therefore conducted using this group of learners to evaluate the effectiveness of the pedagogically valid game.
The effectiveness of the game could be measured by whether it had had an impact on learners’ subject-specific knowledge. Thus, the researcher needed to measure learners’ knowledge at the various game-play stages (pre-play, post-play, and an extended post-play).

As the target audience was vulnerable in nature, the researcher did not interact directly with learners. For this reason, no surveys or interviews were conducted with learners by the researcher. Instead, the researcher provided teachers with a set of informal assessments that could be used in the lessons which made use of the game. Tracking the answers, the learners gave in these assessments would aid in measuring their knowledge on the subject-matter during the specific stages of the game play during the lesson. The assessments and the implementation procedure followed in lessons in which the game was played were given to the teachers. The teachers at the target schools then incorporated these game assessments and procedures into their regular teaching.

As part of the research procedure, the teacher was asked to conduct a play session using the password security version of the “Snakes and Ladders” game. The first step required the teacher to ask children to answer the survey before playing or seeing the game (Appendix E). The second step was to allow the learners to play the game. After learners had played the game, the third step of the procedure was the answering of the survey questions a second time by the learners (Appendix E). The children were not allowed to share or discuss their answers while either survey was being conducted. This concluded the measurement of learners’ initial awareness and knowledge of password security and the game’s short-term educational impact.

The researcher then waited six weeks before returning to the school for a follow-up study. In this follow-up visit, the researcher asked teacher to pose rephrased versions of the questions from the first survey to learners (Appendix E). This version of the survey was designed to determine whether playing the games had resulted in learners remembering and (potentially) applying the lessons in the long-term. Supporting data was gathered by the researcher during interviews with the teacher.

The assessment of the game’s effectiveness was conducted after the learners had been exposed to the campaign’s expert presentation.


8.4.2 School AA

School AA was the first high (secondary) school to be visited by the researcher during the invitation phase of Cycle 1’s campaign. A meeting was held between the researcher and the information technology teacher at the school. The teacher was asked to fulfil the role of the campaign’s subject-matter champion at the school. The teacher would lead all campaign-related activities and make use of the campaign’s resources.

At the time of this visit, the researcher provided the teacher with the invitational package only, containing the letter of invitation, the topic-specific flyers each with a single security message, a copy of the cybersafety pledge form and a form to request an expert presentation at the school.

The cybersafety 101 flyer and the cybersecurity game had not yet been printed at the time. These would be posted to the schools later; however, by this time several poster entries had already been received from the school’s learners.

This school chose not to request an expert presentation at the school. The reason given for this choice was that scheduling would be difficult in the class and assembly timetables. The teachers used the materials in life-orientation and computer studies classes for grade 11s.

8.4.3 School BB

This was the second school to be visited by the researcher during the invitation phase of Cycle 1’s campaign. A meeting was held between with the researcher and the school principal. The researcher explained the importance of the campaign and requested the school’s participation. The principal was interested in the school taking part. The principal assured the researcher that the resources would be pinned on classroom noticeboards. The information technology and life-orientation teachers would be tasked with encouraging learners to take part in the competition. This school did not request an expert presentation.

As with School AA, the invitation packet given to the school did not contain the cybersafety 101 flyer or the game. These resources were, however, posted to the school at a later date. At the time of the visit, a single entry had already been received from this school.

The primary school children were therefore the only learners in Cycle 1 who were exposed to the cybersafety 101 flyers and the games. The topics were thus based on all the campaign’s resources at this school. In contrast, the high school learners’ entries were based primarily on the
topic-specific flyers and on their own or their teachers’, perceptions of which topics were most relevant or important.

8.4.4 Competition Judging

Reminders of the competition final submission date were e-mailed to all the schools that had been invited to take part. These reminders also confirmed the date by which the schools would be notified of winners, and the date of the prize-giving.

As far as the competition was concerned, judging commenced once the posters had been submitted. The winners of the contest were determined by a majority vote by a panel of cybersecurity experts. Judges took into consideration the accuracy of the poster’s content, its artistic presentation, and the overall impact of its message.

Initially the researchers planned to divide prizes into primary and secondary school categories. However, many primary school teachers voiced concerns that it would be unfair to compare poster entries by six-year-olds with those entered by 13-year-olds in the primary school category. Thus, during judging, prize categories included topics and took into consideration the entrant’s age.

Section 8.4 described the real-world implementation details of the 2012 SACSAA campaign and poster competition at each participating school. The following section presents the results of the campaign and poster competition, as well as the results of the evaluation of the cybersecurity game at School A.

8.5 Results and Evaluation

This section presents the results of the 2012 SACSAA Educational Campaign and poster competition. Figure 8.13 illustrates the layout of the chapter. It begins by examining the results of School A, followed by a discussion of the results from the two other schools that took part in Cycle 1. School A was the only constant participant, and thus their data were separated from those of the other schools (section 8.5.1). The section concludes with a discussion of the general results of the campaign, based on the data from all participants.
8.5.1 School A

This section presents the findings from School A. Measurements from Cycle 1 include: the number of participants at the school, the number of posters depicting each cybersecurity or -safety topic, the number of posters addressing different categories of device, the degree to which cybersecurity or cybersafety messages were internalised, the number of posters including depictions of the campaign mascot, and finally the evaluation of the effectiveness of the pedagogically designed cybersecurity board game. Each of the measurements taken during Cycle 1 is discussed below. The results from this school and cycle were published in Van Niekerk, Thomson and Reid (2013), (Reid & Van Niekerk, 2014c), (Reid & Van Niekerk, 2015) and (Reid & Niekerk, 2016).

8.5.1.1 Learner participation

This was first year that School A had taken part in the campaign. A total of 94 learners from the school entered the poster competition, each of submitting one poster. The ages of the participants ranged between 6 and 13 years.

8.5.1.2 Posters per topic

The results reflected how many posters focused on each topic. Some focused on one topic, others
on several. This section refers to the percentage of submitted posters that referred to each topic.

Various cybersecurity topics were covered in the resources and by the expert. In order to categorise topics depicted in posters, the themes and topics covered in the cybersecurity resources e.g. the cybersecurity 101 flyer and the expert presentation, were used. Based on the resources, it was expected that several topics would appear on the posters. As the analysis was conducted, topics were identified and grouped. The topics identified as categories were:

- Stranger Danger;
- Social Networking;
- Browsing and Downloading
- Dangers of Online activities;
- Cyberbullying;
- Cyber Citizenship;
- Cyber Crime;
- Information and Password Security;
- Hardware Security;
- Viruses and Malware; and
- Piracy.

The learners based their poster messages mainly on the expert presentation and the cybersafety 101 flyer (Figure 8.5) content. It was decided that these topic categorisations would be used in future campaigns’ poster analysis. If additional categories were identified, these would be added.

Figure 8.14 illustrates the percentage of School A’s posters depicting each topic. The topic covered most was “Information & Password Security”, with 49% (46 of 94) posters depicting relevant scenarios and messages. The second most covered topic was “Stranger Danger” with 40% (38 of 94) posters illustrating this topic. The commonest messages among primary school children was Stranger Danger, or the dangers of divulging personal information online. It is possible that these messages were most frequent as they related to similar, real life dangers to which they were frequently exposed.

---

1 The percentage of posters addressing a topic cannot exceed 100%. However, the sum of the percentages of posters addressing each topic can exceed 100%. This excess can be attributed to the posters’ ability to depict multiple topics.
Chapter 8 Cycle 1: 2012

Figure 8:14 Percentage of School A's competition posters per topic: Cycle 1
Very few children chose to use the message warning against using illegal software or media as a topic for their posters. The least common topic was piracy: no learners explained or warned against piracy in their posters. This category was included and was of interest to the researcher as a result of the lack of correlation between this result and the ratio of coverage in the material. The message against piracy was included in the cybersafety 101 flyer and was covered extensively in the expert presentation.

The researcher cannot explain this avoidance of the piracy topic conclusively. However, it is possible that learners had contrasting views on the topic; for instance, they may have found downloading material etcetera convenient and accessible and thus beneficial to themselves. An informal tally made by School A’s teachers found that the majority of learners had pirated or accessed pirated series, films, music and/or games.

### 8.5.1.3 Posters per Category of Device

The purpose of this measurement was to determine whether children associated campaign messages with a traditional computer, or with a mobile device, or whether they made no distinction between the two types. The content of the resources and expert presentation addressed most platforms. Figure 8.15 illustrates the findings of the analysis.

![Figure 8:15 Percentage of School A’s posters relating to specific categories of device: Cycle 1](image)
Findings revealed that the majority of learners associated the campaign messages with computers rather than all devices. In total, 59% (55 of 94) posters depicted campaign messages related to computers. The remainder were associated with mobile devices (20% or 19 of 94), while 21% (20 of 94) did not distinguish between devices.

The campaign material addressed both computers and mobile devices. However, based on an informal tally conducted by teachers, and the question and answer sessions held during the expert presentation, the majority of younger learners (age 6–11) primarily use and have home and school access to desktop or laptop computers. Many of the children also have access to their parents’ mobile devices from an early age. However, the trend was that learners had their own mobile device only from age 12. This trend may vary in other schools. Since School A’s learners use computers primarily at home and at school, material that related to computers was more relevant to their existing knowledge. The children who associated the messages with mobile devices or did not distinguish between the two types were mainly older (ages 12–13). Changes to the educational resources were not considered necessary as the content and learners’ activities were similar.

8.5.1.4 Internalisation of Cybersecurity or Cybersafety Message

This measurement aimed to determine how well learners had internalised the message(s) represented in the posters. Analysis of text and images used by learners to convey and/or explain their cybersecurity or cybersafety messages provided information on their demonstrated internalisation of these messages. Figure 8.16 shows the internalisation levels for all the learners from School A.

The majority of learners had internalised the cybersecurity campaign messages, with only 7% (7 of 94) failing to do so. The initial analysis found that the majority of learners (52% or 49 of 94) had fully internalised the campaign messages illustrated in their posters. A further 27% (25 of 94) of learners rephrased the messages provided by the campaign. These learners did not demonstrate that they had fully understood the message. However, they did show some insight into the message and may have begun to relate it to a context or device they understood. Finally, the remaining 14% (13 of 94) of learners presented the cybersecurity or cybersafety messages exactly as the resources and expert presentation had described and explained them. These learners had only begun to internalise the messages, and had not interpreted them but merely reproduced them verbatim.
Figure 8.16 How well School A’s learners internalised the cybersecurity or cybersafety messages: Cycle 1

8.5.1.5 Presence of mascot or logo

This measurement was intended to establish whether the inclusion of a mascot and logos in the material assisted in in Cycle 1 to have been exposed to the Cyber Sid mascot for any length of time, as the mascot and the logo was repeatedly included in the expert’s presentation material. Cyber Sid was introduced to learners as a formal representative of the SACSAA campaign. Through this introduction, learners’ attention was specifically directed to the mascot when discussing the topics. Other participating schools may only have noticed the mascot on the topic-specific flyers and the pledge forms; the teachers did not actively bring either brand or mascot to their attention.

The aim was to measure whether learners had noticed and depicted the mascot or logo in their posters. This might indicate whether learners associated the mascot or logo (brand) with the cybersecurity or cybersafety messages. Figure 8.17 shows the results of the measurement of the presence of the mascot and logo on the posters.

The analysis found that 31% (29 of 94) of the posters had included the mascot or logo. Of these 31%, 20% featured the Cyber Sid mascot, 10% the SACSAA logo and 1% (1 of 94) had used
both the mascot and the logo. In several cases, where the Cyber Sid was included, the message stated that the Cyber Sid would protect you against the dangers of cyberspace and was a “cyber friend”. This indicated that learners were associating the mascot with the cybersecurity or cybersafety message and themes. The logo was unexplained when it was present, although its inclusion indicated that the learners had taken notice of it.

![Percentage of School A’s posters depicting branding symbols: Cycle 1](image)

Figure 8:17 Percentage of School A’s posters depicting branding symbols: Cycle 1

The remaining 69% (65 of 94) of School A’s posters did not include the robot mascot in the poster design. Although most learners did not include the mascot, it was a positive sign that some learners had depicted the mascot or logo at all after a single campaign cycle. An issue of interest for Cycle 1 was whether specific introductions to the mascot and its inclusion in expert presentations use of the mascot awareness of the mascot. The other two schools had not had been given specific introductions to the mascots.

Overall, these findings indicate that learners did notice the branding (mascots and/or logo). In addition, they associated the branding with the cybersecurity or cybersafety messages. These findings support the assumption that the inclusion of the logo and/or mascot can aid in creating a brand identity for the campaign.

The four categories of results discussed above were used to assess the effectiveness of the cybersecurity and safety education campaign. During Cycle 1, a separate analysis of the measurement of the effectiveness of a cybersecurity educational game designed to be
pedagogically sound was conducted. This game an educational component of the campaign. The next part of this section will present the results of the evaluation of the case study at School A.

8.5.1.6 Results of the evaluation of pedagogically sound cybersecurity education game

This measurement was intended to determine whether playing the educational “Snakes and Ladders” cybersecurity game had influenced learners’ knowledge of cybersecurity. If it had had a positive effect on their knowledge, then the game would be considered an effective education tool and SACSAA could continue to use it as part of the campaign’s educational resources. This section presents the results of the evaluation of the game, based on the procedure described in section 8.3.4.6 and Appendix E. These results were published in Reid & Van Niekerk, (2013a) and Reid & Van Niekerk (2014b).

Figure 8.18 shows the percentage of learners who answered the assessment questions correctly in the pre-play assessment, the post-play assessment, and the follow-up assessment. Appendix E provides the wording of the questions in each assessment. In numerical order, each assessment’s questions dealt with the following cybersecurity password management messages:

1. Never write your password down.
2. Trust your parent or guardian with your password.
3. Use combinations of alphanumeric characters and special characters to construct passwords that cannot be easily guessed i.e. not words such as names or places.

The results of the pre-play assessment of learners’ knowledge revealed that some learners did have an awareness of the need for password management. The findings were that just over half (55 %, 6 of 11 learners) knew not to record their passwords, while 64 % (7 of 11) knew how to devise a strong password. Therefore, some learners had a basic knowledge of password construction and confidentiality. However, thorough understanding of confidentiality practices necessary for children was not fully developed. Only 45% (5 of 11) of the learners knew not to share their password with anyone besides their parents. Overall, these learners demonstrated only a beginner’s level of awareness of information security. This limited understanding could be partially attributed to the awareness talks that had been presented by experts who visited the school earlier in the year.
The post-play assessment results showed a significant improvement in learners’ awareness levels. The percentage of learners who answered the security knowledge questions correctly increased in each question (Figure 8.18). Immediately after playing the game, 91% (10 of 11) learners in School A’s grade 5 class, knew not to record their password; 73% (8 of 11) knew to share their password only with their parents; and 82% (9 of 11) knew how to create a secure password.

Overall, the increase in correct responses to all questions in the post-play assessment indicates that awareness had risen among learners after playing the game. Based on these results, a tentative conclusion was reached that the brain-compatible information security game was an effective method of educating children about information security. However, this conclusion did not necessarily hold beyond short-term memory after play. A follow-up assessment would evaluate its effectiveness in relation to long-term impact on learners’ knowledge.

The results of the follow-up assessment revealed that playing the educational cybersecurity game had a long-term impact on the learners’ knowledge. The percentage of learners who answered the assessment questions correctly rose from those of the post-play survey. In the follow-up assessment, 100% (11 of 11) learners knew not to record their password; 91% (10 of 11) knew
to share their password only with their parents; and 100% (11 of 11) knew how to create a secure password.

At the start of the study, teachers had been instructed not to allow learners to replay the game between assessments. They had also been asked not to expose learners to any other educational material dealing with cybersecurity. The teachers reported back that they had followed these requests. Thus, the rise in the results is not attributable to unmonitored, repeated exposure to the educational game or to other material. The increase in the percentage of learners answering correctly may correlate to the learner’s further or delayed cognitive processing of material. On the other hand, it could be attributed to the learners having discussed the game and its lessons amongst themselves after playing and completing the post-play assessment.

Overall, the study found that the game had a positive effect on learners’ levels of knowledge of the relevant cybersecurity or cybersafety messages. The assessments showed that the game had affected the majority of learners’ knowledge both in the short-term (immediately after playing the game) and in the long-term (after a period of time had elapsed). Feedback received from the teacher involved revealed that learners had shown an increased level of awareness of the need for password management. According to the teacher, in the period between the post-play and follow-up assessments, learners had asked further questions and had indicated that they had adopted the recommended behaviours.

The results of the game evaluation conducted as a case study at School A was presented at the “Kaspersky Cybersecurity for the Next Generation” Student Conference: Asia-Pacific & MEA in Singapore. Feedback was sought from delegates and cybersecurity experts during follow-up discussions. This feedback indicated that the experts considered the results of the case study to be promising and believed that the game had potential for use in educating children about cybersecurity. However, these experts did recommend that further studies be conducted using other participants, particularly other age-groups. Such a study should try to prove that the game was consistently successful at educating learners about cybersecurity and show that it was suitable for all age groups.

This section presented the results of the action research process for School A’s data in Cycle 1. The following section presents Cycle 1’s campaign results for the other schools participating in the 2012 SACSAA campaign.
8.5.2 Other Schools

The results of the other schools were analysed separately, as School A was the only school to commit to planned annual participation, and had thus been exposed to all changes made to the campaign. The schools discussed in this section may continue to participate however it cannot be guaranteed that this will be in consecutive years. The results from this school and cycle were published in (Reid & Van Niekerk, 2014c).

Cycle 1 presents the results for School AA and School BB. These are both high schools that opted to take part in the SACSAA educational campaign and the poster competition. These children were older than those at School A. Each of these schools experienced the same implementation (section 8.4.2 to section 8.4.3) and received the same educational resources; both declined expert presentations and teachers’ self-reported actions taken in the use of the materials in their classrooms were identical. As a result of these similarities, their results are discussed together.

The Cycle 1 measurements to be discussed for these schools, like School A, include the:

- number of participants from the school,
- number of posters depicting each cybersecurity or -safety topic,
- number of posters addressing each category of device,
- degree to which the cybersecurity or cybersafety messages were internalised,
- number of posters including depictions of campaign mascot and logo.

Neither of these schools were exposed to the pedagogically designed “Snakes and Ladders” cybersecurity board game.

8.5.2.1 Learner participation

This was School AA’s and School BB’s first year taking part in the campaign. A total of 122 learners from School AA and a single learner from School BB participated. Their participation in the SACSAA campaign’s cybersecurity poster competition was completely voluntary. More learners from School AA were interested in taking part than at School BB. The difference in participation could not be explained by the researcher. It may have related to time-constraints or other commitments, which deterred School BB learners from taking part.
Learners submitted one poster each. The posters illustrated how each of the learners understood one or more of the campaign’s cybersecurity topics. The age of participants from School AA and School BB ranged from 13 to 18 years.

8.5.2.2 Posters per topic

This section presents the percentage of the posters illustrating each topic (Figure 8.19). Learners could choose one or more topics to include on their posters. Of all the resources and content, the schools had been given and on the implementation procedures, learners chose to use cybersecurity or cybersafety messages taught by the topic specific flyers (Figure 8.2) and by messages which the teacher emphasised.

The majority of learners from In School AA illustrated cybersecurity or cybersafety messages and lessons relating to cyberbullying. A total of 48% (58 of 122) of the posters featured cyberbullying as a topic. This shows that the topic was particularly relevant to these learners or considered particularly important. The second commonest topic was “Information and Password Security”. This topic dealt with password management and the protection of confidentiality and availability of the learner’s personal information. This topic was featured on 24% (29 of 122) of the posters.

The third most frequent topic was cybercrime, with 22% (27 of 122) of the posters including messages referring to this topic.

The commonest topics dealt with issues that learners would be expected to relate to because of their age and their status as digital natives. Based on an informal tally conducted by School AA’s teacher, the majority of learners at this school had access to or owned their own mobile phone/device. Learners were active on various social and gaming sites, and were conscious of the importance of keeping their personal information private. When using both types of device, using apps and online, learners were conscious of the need for strong passwords and their good management. In relation to cyberbullying, the teacher reported that many of the students had indicated they were aware of or had experienced cyberbullying in their own social networking activities. It was interesting to note that the illustrations of cybercrime suggested that learners did not want to become victims of cybercrime. Phishing was the most commonly illustrated crime. It was mentioned in both the content of topic-specific flyers (explicitly) and in the cybersafety 101 flyer (by example). Learners’ stance on committing criminal acts was less measurable than their stance against becoming victims.
Figure 8:19 Percentage of Other Schools’ competition posters per topic: Cycle 1
Topics that did not feature on posters from learners at School AA were “browsing and downloading”, “dangers of online activities”, “hardware security” and “piracy”. These topics may have been rejected because they involved messages that might inhibit or inconvenience the learners in their online activities. Several learners indicated that they did not want to be victims of cybercrime; however; none indicated that they were against piracy. Piracy is a crime. This could indicate that learners were against cybercrime but that at the same time they rejected the campaign’s view that piracy and infringement of other entities’ property rights should be stopped. This stance seemed to be linked strongly to if learners received benefits from such infringements.

A minority of the posters depicted other topics. Firstly, social networking was an issue of interest that was depicted on only 17% (21 of 122) of the posters. Both the topic-specific flyers and the cybersafety 101 flyer covered social networking issues and security and safety practices. The learners’ illustrations of the topic typically provided either an example of cyberbullying and a message to stop or report it, or advice on what to do if they or someone known to them experienced cyberbullying. Secondly, stranger danger was depicted by 10% (12 of 122) of the posters. This may be attributable to the content of this message being targeted specifically at primary school children, although it remains a concern among this age group. Most of the posters which featured stranger danger messages also featured social networking messages. Thirdly, 11% (14 of 122) of the posters covered the topic of viruses and malware. The topic-specific flyers and the cybersafety 101 flyer covered the topic of viruses and malware. Learners’ illustrations of this message generally mirror exactly what learners read in the resources. However, a few learners did contextualise their drawings and explain the messages in their own words. Unlike School A, the messages were not restricted to the need for antivirus applications and firewalls. Finally, the last topic which was largely ignored was cyber citizenship. Only 2% (3 of 122) of the posters used this message. Poster content related mostly to netiquette and contributions to online bodies of knowledge, e.g. forums, discussion boards and question and answer pages.

Although School AA and School BB experienced similar implementations of the campaign, School AA learners were more willing to take part than those at School BB, as indicated by the participation rate. This section now briefly describes the entry from School BB.

The single entry from School BB (100% of the posters) carried anti-virus and malware cybersecurity or cybersafety messages. The message aligned perfectly with the SACSAA campaign’s message. The learner had drawn inspiration from the topic specific flyers but had internalised the message and related it to his or her own circumstances. The poster depicted
viruses and their effect on the learner’s files and activities. It also recommended the use of an anti-virus program and a firewall.

8.5.2.3 Posters per Category of Device

The measurement aimed to determine whether learners associated the campaign’s cybersecurity or cybersafety messages with a particular device or whether they adapted the message to multiple devices.

Most of the learners who took part from School AA associated the campaign’s cybersecurity or cybersafety messages with both traditional computers and mobile devices. Overall, 85% (104 of 122) of the posters depicted the messages as applying to multiple types of devices (making no distinction between devices). The remaining posters were divided in their association with particular devices. Of the remaining posters, 11% (13 of 122) related their messages to computers. The posters related to the use of firewalls and antivirus programs (the “viruses and malware” topic) and the prevention of access via the use of a password (the “information and password security” topic). On the final group of posters (4% or 5 of 122) the messages were associated with mobile devices. These posters mainly carried social networking messages and cyberbullying messages.

The learner from School BB associated the virus and malware message with a traditional computer. The poster carried an illustration of a virus or malware attempting to infect a personal computer, with an anti-virus application and a firewall defending the computer against the threat. In the text the example was explained in the context of a desktop computer.

Overall, the findings from these two schools were similar. The majority of learners did not associate their cybersecurity or cybersafety messages exclusively with a particular device. They adapted the messages to suit the various devices that they made use of and illustrated in their posters. Based on the analysis of the data, it was not deemed necessary to alter the cybersecurity education material to make specific associations with all devices. The learners had shown an ability to interpret the examples and to contextualise them, making them more relevant to their own circumstances.

The findings from Schools AA and BB contrasted with those of School A. Both schools discussed in this section were high schools. A comparison with the results from analysis of the primary school’s message-device association is provided in section 8.5.3.3.
8.5.2.4 Internalisation of Cybersecurity or Cybersafety Message

This measurement aimed to indicate how well learners had internalised the 2012 SACSAA campaign’s content message(s). It analysed their depictions and explanations of the topics selected for inclusion in their poster entry.

The majority of the posters (93%, 114 of 122) from School AA reflected that learners had fully internalised the messages they had depicted in their posters. Their depictions and explanations of the various cybersecurity topics indicated that they had contextualised the messages in relation to the circumstances, activities, and platforms they were familiar with.

The remaining learners had also internalised the campaign’s cybersecurity or cybersafety messages, but to a lesser degree\(^2\). Of the remaining posters, 3% (4 of 122) from School AA indicated that learners had internalised the campaign message to the point of rephrasing the message. The examples and explanations used to explain the cybersecurity or cybersafety message were adapted to use examples learners could relate to and explain in their own words.

A final 3% (4 of 122) of School AA’s posters showed that a few learners had achieved only a limited internalisation of the campaigns messages. This group of posters indicated that learners had illustrated and explained their chosen cybersecurity or cybersafety messages as these had been taught. In these cases, the posters made use of the same examples and phrasing as the topic-specific flyers and cybersafety 101 flyer, which had been provided as educational resources.

In terms of this measurement, the material was effective for School AA in raising learners’ cybersecurity awareness levels. The educational resources proved successful in that learners were now able to reflect on the lessons learnt and fully internalise the messages in relation to themselves or familiar situations or contexts. The material also proved effective for the learner from School BB; however, since there was only one submission from this school no further comparisons could be made.

---

\(^2\) During the final analysis of the entire campaign’s history it was noted that Cycle 1’s result of having all learners internalize the material to some degree was an anomaly. Future cycles were more indicative of the effective of the campaign on multiple audiences.
8.5.2.5 Presence of mascot or logo

This measurement was intended to establish whether the inclusion of a mascot and logos in the material aided in the creation of a memorable brand for the campaign amongst the learners. Both the mascot and the logo were present in the majority of the educational resources which were provided to the schools as part of the campaign. School A had had an expert presentation where the mascot had been introduced to learners and incorporated into the presentation. School AA and School BB had both opted not to have such a presentation. Therefore, these learners had not been introduced to the mascot and were unfamiliar with its backstory and its relevance to the campaign. Therefore, it was anticipated that the measurements from these schools would indicate whether learners had noticed the mascot and logo on the topic-specific flyers and the pledge forms and assigned some level of importance to them.

None of the learners from either School AA or School BB included the mascot or the SACSAA logo on their posters. The results of this measurement for School AA and School BB can be interpreted several ways.

Firstly, this absence of mascot and logo may indicate that none of the learners noticed the branding. Lacking active specific introduction to the mascot, learners may have been unable to relate to the mascot and/or associate it with the cybersecurity or cybersafety messages.

The second reason for the lack of inclusion of the branding by these learners relates to format of the submitted posters. School A’s poster entries were hand-crafted, thus they had can depict any image they were capable of drawing. In comparison, all the posters form School AA were digitally created. The posters consisted of text, clipart images, and downloaded pictures. The significance of this is that learners may not have been able to find an online copy of the SACSAA logo or of the Cyber Sid mascot without going directly to the campaign’s website. In addition, they may not have known how to copy or recreate the mascot or logo digitally for inclusion in their posters.

The single poster entry from School BB was handcrafted. However, it did not include any branding either. This may indicate that the learner did not notice the branding, did not recognise the branding as being relevant to the campaign’s messages or did not associate the mascot with the topic depicted on the poster.

Overall, these findings are inconclusive. It appears that learners did not notice the branding (mascots and/or logo). However, the absence of branding on their posters may also be attributable to a lack of technical skill or resources with which to copy or replicate the brand icons.
This section presented the results of the action research process for the two high schools that took part in in Cycle 1 of the 2012 SACSAA education campaign and poster competition. The next section presents the general results for this research cycle of the campaign.

8.5.3 General Results

The schools which participated in Cycle 1’s campaign and competition and which have been discussed above were School A, School AA and School BB. This section discusses the general results of the game, examining all the data gathered collectively. The general trends in participation numbers, the number of posters depicting each topic and the degree of internalisation of campaign messages will be discussed.

The first trend was unrelated to the measurements taken: this trend related to the chosen format of the posters. The primary school (School A) decided that learners would submit handcrafted posters, while learners from the high school that submitted most entries, School AA, create their posters digitally. School BB submitted a single, handcrafted submission.

This trend may be the result of high school learner’s greater experience using computers to create digital reports and media. Feedback from the teachers indicated that all projects at a high school level were required to be digitally created or presented. The format in which the posters were created may have affected the measurement of the percentage of posters that included the campaign’s branding (mascot or logo).

8.5.3.1 Overall Participation

This campaign was more successful than its predecessor. A total of 217 poster entries was received. This was an increase of 214 posters over the three that were submitted in the 2011 pilot campaign (Cycle 0, Chapter 7). Primary school learners (School A) accounted for 94 of the poster entries. The remaining 123 entries were received from high school learners (Schools AA and BB); only one of these entries came from School BB, however.

Despite receiving many requests from schools across South Africa for campaign resources and competition flyers, all entries were from the Nelson Mandela Metropolitan area. In fact, all entries were received from schools that had been visited in person by the researcher to advertise the competition and explain its purpose to learners and teachers.
8.5.3.2 Posters per topic

Figure 8.20 below indicates the topics primary school children and secondary school children considered important. It allows a comparison between these broad age groups’ results.

Of the 217 posters submitted, 76% (165 of 217) depicted a single topic, whilst the remaining 24% (52 of 217) depicted more than one. This section examines whether there was a difference between the topics primary school children considered important and those secondary school children preferred. Therefore, School A’s results represent primary school learners, and the joint results of School AA and School BB represent high school learners (Figure 8.20).

The first trend reflected in Figure 8.20 shows that both primary and high school learners related to the topics of cyberbullying and information security. Similarly, both groups showed no preference for the campaign’s anti-piracy messages. Learners may have rationalised piracy to their advantage. It is possible they did not consider stopping the infringement of copyright worth the loss of the benefits of piracy (i.e. access). The expert presentations covered anti-piracy messages comprehensively while the cybersafety 101 flyer mentioned it briefly. Regardless of the amount piracy content that learners saw, the message was not adopted.

The next trend was that a relatively similar percentage of the target audience in both primary and high schools included messages relating to “social networking” and viruses and malware in their posters. Primary school posters including social networking and dangers of online activities topics were mainly submitted by older learners. These learners would probably have been engaging in similar cyber activities to high school learners at this point.

The third trend was that there was a definite difference in adoption of certain topics between the two school levels. Stranger danger, cyberbullying, cyber citizenship, cybercrime and information and password security were all covered by learners from primary schools and high schools. However, primary learners had a higher rate of use of stranger danger messages, cyber citizenship and information and password security. This may be because these messages were similar to other messages, unrelated to cybersafety, that are aimed at this age group.

Stranger danger is a common social issue discussed with children. Just as being kind, helpful and community-spirited are important, an awareness of the dangers strangers pose is a foundational social issue often taught to young learners but not to older ones. The high school posters featured a higher percentage of posters depicting cyberbullying; this issue may be more relevant to this age group.
Figure 8:20 Percentage of all schools’ competition posters per topic: Cycle 1
Topics which were only used in the primary learners’ posters were browsing and downloading, dangers of online activities and hardware security. These topics are primarily covered in the expert presentations, and not explained in the campaign’s printed resources. This trend, and the list of topics which high school learners did depict, suggests that the high school learners primarily drew their messages from the cybersafety 101 flyer. In contrast, the primary school learners learnt lessons from all the campaign resources, including the expert presentation.

### 8.5.3.3 Posters per Category of Device

This measurement aimed to determine whether learners associated the campaign’s cybersecurity or cybersafety messages with a particular type of device i.e. a traditional computer or mobile devices. The discussion of this measurement compares the results from learners from primary school to the those from learners at high school (Figure 8.21).

![Figure 8.21 Percentage of all schools' posters relating messages to specific device categories: Cycle 1](image)

The results of this measurement show a definite difference between primary high school learners. Primary school learners showed a tendency to associate the messages with a single device, in most cases the computer. On the other hand, most high school learners did not associate the message with any particular device.
As discussed above, the primary school children in this study mostly use traditional computers (section 8.5.1.3). Therefore, it was more likely that they would interpret the campaign content in relation to personal computers. The high school learners, however, are familiar with a wider variety of devices. This was reflected in their posters. The educational resources covered the messages in terms of a variety of devices.

Based on the results of the poster analysis and the knowledge of the learner’s users’ habits, the researchers decided it was unnecessary to alter the material so that it focused more specifically on applying the messages to specific devices.

### 8.5.3.4 Internalisation of Cybersecurity or Cybersafety Message

The measurement determined the level to which the learners had internalised the cybersecurity or cybersafety messages they had chosen to depict in their posters. A comparison of the level of internalisation between primary school learners and high school learners is presented in figure 8.22. At both schooling levels, the majority of students had fully internalised the cybersecurity lessons. However, the percentage of students making up the majority at the individual school levels was significantly different.

![Figure 8.22](image)

**Figure 8.22** How well all the schools’ learners internalised the cybersecurity or cybersafety messages: Cycle 1

<table>
<thead>
<tr>
<th>Percentage of posters (%)</th>
<th>As given</th>
<th>Rephrased</th>
<th>Fully</th>
<th>Uninternalised</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary School Learners</strong></td>
<td>14</td>
<td>27</td>
<td>52</td>
<td>7</td>
</tr>
<tr>
<td><strong>High School Learners</strong></td>
<td>3</td>
<td>3</td>
<td>93</td>
<td>0</td>
</tr>
</tbody>
</table>
At the primary school level, the percentage of learners who had fully internalised their depicted messages was 52% (49 of 94); in comparison, the level of learners from high school who had fully internalised the messages was 93% (115 of 122). This may suggest that the level of content was new or moderately challenging for primary school learners, while it was simple or already understood in the case of high school learners.

None of the high school learners failed to internalise the cybersecurity or cybersafety messages, while a small minority of primary school learners had not internalised the messages (7%, 7 of 94). These learners were mainly the youngest learners in the group who probably had limited experience in unsupervised or assisted use of computers or mobile devices.

As most of learners had internalised the material to some degree, the researchers were able to reach the conclusion that the material had taught the learners effectively. The material was designed to comply with the recommendations of brain-compatible education principles. Since it appeared to be having a marked success on educating the learners, a decision was made that future campaign cycles would continue this practice.

8.5.3.5 Presence of mascot

The presence of the mascot or logo on learners’ posters could indicate that they associated the campaign’s messages with the campaign mascot or brand. This would suggest that a campaign brand identity could form amongst these learners. Figure 8.23 shows the percentage of posters that included the campaigns mascot or logo.

Of the 217 poster entries in the 2012 campaign cycle, 9%(19 of 217) included the Cyber Sid mascot, 4% (9 of 217) included the SACSAA logo and 0.46%(1 of 217) included both the mascot and the logo. The overall measurement was low, showing that although some brand awareness did develop it was among the minority of the campaign participants.

The differences in implementation of the campaign at the schools resulted in the mascot and logo being introduced to the learners in different ways. The implementation differences regarding the branding and their effect on the adoption of the branding symbols by learners became an issue of interest.

The mascot was introduced to primary school learners in a direct manner; it mascot was introduced as a character, his ‘backstory’ as a cyber-guardian was provided, and he was included
in explanations and discussions. The campaign logo was also highlighted as being part of the campaign. The high school learners received no direct introduction to the branding symbols. They were left to notice the branding (mascots and logos) on the educational resources.

![Figure 8:23 Percentage of all schools' posters depicting branding symbols: Cycle 1](image)

When taking into consideration the different approaches to introducing the mascot to learners, it can be posited that how learners are introduced to the branding may affect their awareness of these branding symbols.

How the branding was introduced or explained to learners had a definite impact on their adoption of the mascot and logo. The primary school learners, who had been introduced specifically to the branding, adopted it to some degree: 20% (19 of 94) of the learners depicted the mascot on their posters, 10% (9 of 94) of the learners included the SACSAA logo and 1% (1 of 94) of the learners used both the mascot and SACSAA logo. In comparison, none of the high school learners (0 of 123) included either of the branding symbols in their posters.

One possible reason for high school learners ignoring the mascot is that they felt they were “too cool” or “too old” to include it. This reason could possibly apply to older primary school children also. Another possible reason is that this difference in the results is related to differences in the campaign’s implementation of the introduction of the branding to learners. However, the
difference in results may also relate to the different formats used by learners when creating their posters, as discussed in section 8.5.3. The primary school learners submitted hand-drawn posters, while high school learners submitted digitally created posters. The primary learners were free to depict anything they were capable of copying, imagining, and drawing. Theoretically, the high school learners could also create anything they visualised. However, a broader range of technical skills was required, depending on how they chose to create or copy the images. The absence of branding symbols may be related to both to a lack of awareness of the branding symbols, and a lack of technical skills to depict them. Future cycles should continue to monitor the implementation of the campaign, the introduction of mascots and logos and the effect on the campaign’s brand association.

This section presented the general results from Cycle 1 of the action research process for all the schools participating in the 2012 SACSAA education campaign and poster competition. This concludes the results section for Cycle 1. The next section presents the researcher’s reflections on lessons learnt from this research cycle of the campaign.

## 8.6 Reflections

This section discusses reflections and lessons learned from the implementation of the SACSAA campaign, Cycle 1, in 2012. Some of these lessons relate to the actions taken in attempts to address problems identified at the beginning of Cycle 1. Other lessons were learned in the implementation of the campaign. This section first addresses the lessons learnt as a result of actions taken to meet Cycle 1’s objectives, and then outlines additional lessons learnt.

C1O1 was to:

"Establish a more formalised education approach with supporting materials which are pedagogically sound."

The first action taken to meet C1O1 was to provide educational activities and resources that were separate from the competition. The competition continued to serve a minor educational role in the campaign; however, its primary purpose became the measurement of the effect the other educational resources had on learners’ knowledge.

The second action taken to meet C1O1 was the pedagogical design of the campaign’s now separate educational activities. The educational component of the campaign involved the provision of supporting material (section 8.3.2), which was more formalised from an educational
Chapter 8 Cycle 1: 2012

perspective. Literature has shown that many information security educational efforts have neglected deliberate compliance with a pedagogical theory (Puhakainen, 2006). This campaign aimed to design its material by taking into consideration the recommendations of a pedagogy that was suited to its broad audience and its intended educational resources. The design of the education component of the campaign complied with brain-compatible education principles. This included the design and use of the educational resources.

The campaign’s educational content was designed to tie in with brain-compatible educational (BCE) principles. This presentation style was used to make the material as appealing and as easy to learn as possible for as many learners as possible. The BCE pedagogy caters for a variety of age groups, a variety of learning styles and involves the implementation of formal education strategies. Its application correlates with learners generally high rate of internalisation of the messages in Cycle 4 of the campaign. Regardless of the exact campaign implementation, all learners saw some or all the brain-compatible educational material. Exposure to a brain-compatible presentation was therefore a constant in the study.

Cycle 1’s first lesson learnt while meeting C1O1, and the sixth lesson in the entire research process, was that:

Lesson 6

_providing distinct educational and evaluation components in the campaign provides learners with more opportunities and experiences from which they may learn the campaign’s intended teachings._

Cycle 1’s second lesson was that:

Lesson 7

_Designing and implementing the campaign and its materials in order that it complies with pedagogical principles can positively affect a learner’s educational experience and improve the campaign’s probable effectiveness._

Both lessons indicate that future cycles of the SACSAA campaign should continue to implement the design and implementation practices.

C1O2 was:

“To increase school and learner participation, by actively campaigning and advertising the campaign and competition to attract interest and participation.”
The first action taken to meet C1O2 was the continuation of the practice of sending out invitations to participate via the postal services and including campaign information on the SACSAA website. This action was, however, only the start of the advertising and motivation process of this campaign.

The second action taken to meet C1O2 was making visits to schools to explain the purpose of the campaign and to invite the schools to encourage their learners to take part. No poster entries were received from schools that were not visited in person. Even schools that requested information via the mail did not take part without an official visit being made. This indicates that issuing personalised invitations and having an active representative visit schools in an official capacity was particularly effective in convincing schools to encourage their learners to participate and benefit from the campaigns teachings. The third lesson learnt from Cycle 1 (Lesson 8), relates to Lesson 3. Lesson 8 was that:

**Lesson 8**  
*personalising official communication and interaction with the schools and target audience correlates with increased interest and participation in the campaign effort*

During the school visits the researcher explained the campaign to the school principal and/or the teacher chosen as school liaison. Schools tended to select their information technology and/or life-skills orientation teachers to communicate with the campaign representative and implement the campaign at the school. All schools taking part were those which had received personal visits. Schools where the researcher met with the school principal and the teachers involved had the highest rate of participation (School A and School AA). The third school, where the researcher had only met one teacher had a lower participation rate. Based on this experience, the following lesson was learnt:

**Lesson 9**  
*Obtaining principal and teacher commitment to participation and subscription to the campaign and its messages contributes to the implementation and support of competition at the school.*

This lesson is similar to what has been found in organisations where top management support assists in information security efforts (Kankanhalli, Teo, Tan, & Wei, 2003; S. H. von Solms & Von Solms, 2004).
Following the advice of a marketing professional on how to incorporate branding, the third action to meet C1O2 was the inclusion of brand symbols (the Cyber Sid mascot and the SACSAA logo) to provide images with which learners could associate the campaign’s messages (section 8.3.2). This brand-association could be used to remind users of the cybersecurity campaign and its messages in the future. The branding would make the campaign more relevant to learners.

According to the findings from Cycle 1, it is clear the type of brand symbol selected is important, and how it is brought to the attention of learners may affect its adoption. The Cyber Sid mascot was depicted more often than the SACSAA logo, suggesting that a character-based branding may be more appropriate to the learners. However, character mascots may not be suitable for all age groups. The learners who depicted the brand symbols were from schools that had deliberately and directly introduced to the symbols.

Lesson 10 of the research process was that:

Lesson 10

*Branding elements should be carefully designed and actively incorporated into the campaign if they are to be related to the cybersecurity or cybersafety messages.*

This lesson may be confirmed in the next cycle. Cycle 1 showed that learners do not notice branding. Future cycles may need to establish how memorable the brand is in order to establish whether a brand association or brand identity can be established. Researchers may also examine whether brand symbols were more appealing to a particular group of learners.

The fourth action taken to meet C1O2 was the advertisement of prizes for the winners of the competition. These prizes served as an incentive to encourage participation by attracting the learner’s attention. The lesson learnt from this action will be will be outlined in the section discussing actions taken to meet C1O3.

The final actions taken to advertise and attract participation was media coverage of the campaign by local newspapers, radio stations and the SACSAA website. Several interviews and information sharing sessions were held. The resulting media coverage of the campaign assisted made schools and the general public more aware of the cybersecurity education effort. Several schools requested the information packages when they became aware of or gained trust in the campaign from the media campaign. Most of the schools who requested the materials received the educational resources and made use of them to some extent. However, they did not take part in
the campaign’s poster competition, thus the effect the campaign had on them could not be measured. As a result, these schools could not be included in the research report.

Mass media can reach a larger target audience than individual campaign implementations. Making use of the media to share the message of the campaign assisted in making many schools and individuals aware of the campaign, its website and cybersecurity as an issue. This demonstrated that making use of existing resources such as communication and advertising channels can benefit a campaign.

Having experts in the field of communication and advertising promoting the campaign resulted in raised awareness of the campaign. The influence of experts was particularly apparent in the advertising choices and brand symbol design and use. The campaign experts are primarily specialists in cybersecurity content and thus design decisions relating to marketing, educational design and delivery could all be better implemented by subject-specific experts. It can be hypothesised that expert contributions would result in the relevant element(s) of the campaign being more successful. If its sub-components were more successful, the campaign as a whole would in all probability be more successful. This consideration led to Lesson 11 which will continue to be explored in future campaign cycles. Lesson 11 was that:

**Lesson 11**

*The use of existing resources and experts should be encouraged where possible, as a cybersecurity campaign is a multidisciplinary endeavour.*

Overall, the collective actions taken to meet C1O2 showed that Lesson 2, initially identified in Cycle 0, is valid. There was a relationship between increased levels of participation and increased, continuous effort to market and make people aware of the campaign and its messages.

C1O3 was to:

“*Simplify the implementation of the data collection method used for evaluating the campaign’s effect on learners.*”

In order to meet C1O3, the guidelines and submission formats for the poster competition were redefined. Only posters were admissible, and the video category was discarded. This significantly decreased the number of formatting and technical queries relating to the creation of submitted work and made the measurement simpler to implement and maintain. Thus, Lesson 5, previously identified in Cycle 0, was confirmed and C1O3 was fulfilled. However, a few new issues related
to the implementation of the evaluation method were discovered while analysing the posters from Cycle 1. These issues are listed and discussed briefly below.

1. **The format of a poster could affect the branding measurement**

   Posters could be submitted in hand-drawn or digital formats. A concern arising from analysis of the entries was that the digitally created posters may have skewed results in relation to the measurement of the presence of brand symbols. During analysis, it was hypothesised that the absence of these symbols on the digital entries may have been the result of a lack of technical skills to find or recreate the images.

   This observation led to *Lesson 4* being relearnt. A sub-lesson learnt in Cycle 1 was that it is necessary to:

   **Sub-lesson 4B**

   Ensure that the implementation of the evaluation method is suited to or takes into consideration the skills (technical and non-technical) of the audience being investigated.

   Future campaigns should provide access to mascot and logo images in a digital format to reduce the chance of these being excluded because of a lack of technical skill on the part of the learner. Hand-drawn entries should be encouraged, particularly among those less technically skilled learners such as junior primary (grade 0 – grade 3) learners.

2. **Poster creation criteria are required to enable fair judging and content analysis**

   This second issue aims to ensure that measurements taken within the content analysis are comparable. The posters formed the data selected for analysis of the campaign’s effect on the target audience. In order to compare results, it was important that the data were in a comparable form.

   All submissions were required to meet broad characteristics of what researchers regarded as an awareness-raising poster, i.e. a poster should contain a cybersecurity or cybersafety message with supporting or explanatory images, a balance between of text and images and so on. Therefore, in addition to providing access to campaign branding images and encouraging hand-drawn entries, the campaign should stipulate the requirements for a poster. This guidance could also be used as preliminary judging criteria.
3. **Poster criteria are needed to prohibit submissions from duplicating campaign materials or infringing other resources’ copyright**

The poster guidelines discussed above would prevent the generic entries. Apart from measuring the learner’s knowledge after exposure to the campaign, the intention of the poster campaign was to use the best poster entries as awareness-raising materials in future campaigns. Material which was inappropriate on a poster, or too generic, or which violated copyright could be used.

Many of the entries from the high schools were text heavy and formatted as awareness-raising brochures rather than awareness-raising posters. In addition, most of the digital entries had been “cut and pasted”. Few learners who submitted digital entries created completely original works. Therefore, the researchers agreed that hand-drawn posters provided a better indication of true assimilation of the subject matter.

4. **Prizes should be pre-allocated to judging criteria**

This fourth issue related to the evaluation method used in the poster competition the selection of prize winners. Initially, the researchers had planned to have only two prize winners, a primary school winner and a high school winner. However, many primary school teachers expressed concerns about the lack of fairness in comparing poster entries by six-year-olds with those by 13-year-olds. The level of content differed according to age, experience with technology and understanding of the campaign. Therefore, additional categories were devised, with prizes.

Prizes were intended as incentives to encourage learners to participate in the competition. Feedback from several teachers indicated that prizes did attract their learners’ participation. Based on this feedback, the researchers agreed that clear criteria for winning and awarding prizes in several categories may further encourage learners to take part. Therefore, the lesson learnt was that:

**Lesson 12**

*Incentives to encourage participation should be well-defined, thoroughly explained at the start of the effort, and be fairly allocated.*

An issue of interest to examine in forthcoming iterations is whether the value of the prize affects the learner participation rate.
This concludes the discussion of lessons learnt in relation to the Cycle 2’s objectives d. There are, however, other reflections and lessons that have been learnt. These are discussed below.

The first reflection, which is not related to an objective, is a confirmation of the previously outlined Lesson 11. The lesson encourages the use of existing resources. It was found that teachers in their supportive and representative role at the schools were vital in promoting the campaign among their learners. Teachers’ use of the provided materials and their support of the campaign encouraged learners to develop an awareness of cyber issues and to participate in the campaign. This level of interaction went beyond the boundaries of any interaction a campaign expert would have had with the target audience. Added to this, teachers have a better skillset for teaching than the campaign’s content experts. Therefore, it is hypothesised that teachers play a vital role in the education campaign. More active participation from teachers would be an issue of interest in future campaigns. All the teachers in this cycle provided feedback, emphasising that they would be willing to become more involved in the campaign’s implementation at their schools if they had sufficient resources.

The second reflection that is not related to an objective supports Lesson 3. Part of making the educational approach more engaging was the fact that the campaign followed brain-compatible (BCE) principles. This stemmed from C1O1 and C1O2. Personalising and contextualising the educational content for the learners was undertaken to meet the objectives and to follow BCE principles. This was done chiefly in the expert presentation.

Many of the learners internalised the messages to some extent. However, posters submitted by School A that had been fully internalised were considerably more contextualised in their depictions of the explanations of the cybersecurity concepts. This may relate to the fact that they had heard an expert presentation in which they were encouraged to apply the concepts to contexts with which they themselves were familiar and which may not have been explicitly covered by the materials or presentation. This provides the starting point for the formation of Lesson 13, that is:

**Lesson 13**

*Personalising and contextualising the campaign and its resources to suit the needs of the target audience can correlate with an increased level of internalisation*

The lesson is explored further in subsequent cycles.
The final reflection that is not related to an objective relates to the distribution of the campaign content as opposed to the cybersecurity content messages adopted by the target audience.

Cycle 1 found that learners showed definite trends in topic preferences; e.g. cyberbullying was commonly depicted, while anti-piracy messages did not feature. The messages were covered in the same or similar depth in the material. However, the adoption rate of these messages was not equal. Both issues were relevant to the audience, but attitudes towards the issues appeared to be different based on the numbers of posters depicting the messages.

Future cycles should examine whether coverage of campaign content commensurate with the severity of the issues would have an effect on the learner’s adoption of a message. For example, cyberbullying is commonly experienced and/or perpetrated by learners. Similarly, learners may either pirate material or have easy access to pirated material. Both actions are commonplace, wrong, but probably more likely to be experienced by learners than an issue such as serious cybercrime. The question thus arises: should these topics be covered in more detail than topics such as cybercrime? Would this have an impact on the adoption rate of the messages? Subsequent cycles examined this issue.

8.7 Conclusion

Overall, Cycle 1 improve upon the pilot of the SACSAA cybersecurity and safety awareness campaign and competition in 2012. Participation increased significantly. Both primary and high school learners took part. This was the first year that researchers were able to analyse data comprehensively. This analysis led to several lessons being learnt. These lessons learnt within Cycle 0 and Cycle 1 were taken into account in the subsequent, second official campaign iteration.
Chapter 9 Cycle 2: 2013

9 Action Research Cycle 2: 2013

Introduction

Description of the Context

Chapter 2
Information Security and Cybersecurity

Chapter 3
Information Security and Cybersecurity Education

Methodology

Development and Detail about the Selected Issues

Chapter 5
Theoretical Basis of Action Research Interventions

Action Research Process

Chapter 7
Cycle 0: Pilot

Chapter 8
Cycle 1: 2012

Chapter 9
Cycle 2: 2013

Chapter 10
Cycle 3: 2014

Chapter 11
Cycle 4: 2015

Chapter 6

Conclusion
This chapter presents Cycle 2 of the action research process. Cycle 2 examines the interventions conducted on the SACSAA cybersecurity and cybersafety in 2013. This cycle focused on introducing continuing to consider pedagogical principles in the design and implementation of the campaign. It also investigating the effect of contextualising campaign content and emphasizing messages to different degrees.

9.1 Introduction

Cycle 2 was the second official implementation of the campaign and competition. It was focused on continuing the successful practices from previous campaign cycles while at the same time adjusting the campaign in areas that had not been successful. Cycle 2 continued the application of pedagogical practices discussed in 2012, and aimed to improve the campaign’s relevance to the target population. The following sub-sections outline the details of the cycle. The iteration is presented according to the layout shown in Figure 6.2. This was the third iteration of five action research cycles and campaign years included in the thesis. The following sections describe the design, implementation, and results of Cycle 2.

9.2 Problem Identification

In Cycle 1 it emerged that addressing some of the campaign’s design and implementation issues improved levels of learner participation in the campaign and competition. In addressing issues such as a lack of formalised pedagogical instruction, the campaign had a positive educational effect on most participants.

Cycle 2 aimed to build on the previous cycles’ campaign practices. Thus, it continued to address problems identified in the earlier iterations, while at the same time addressing issues of interest that were identified from Cycle 1’s results. Cycle 2’s issues of interest included:

- the continued need for a more formalised education approach, including more formalised education material and increased involvement of educators (Section 9.2.1);
- the use of effective marketing and procurement of agreement to participate from the schools and the learners (Section 9.2.2);
- the re-evaluation of the effectiveness of the “Snakes and Ladders” cybersecurity game as an educational game for a variety of target audiences (Section 9.2.3).
• the need to increase the relevance and contextualisation of the campaign and its content for learners in order to enhance the education experience (Section 9.2.4);
• the need to determine whether a correlation exists between the content emphasised in the campaign and the content used by learners in their posters (Section 9.2.5).

Each issue of interest, introduced in the past and present iteration, and Cycle 2’s associated objective to address the issue of interest are briefly discussed below.

9.2.1 Establish a more formalised education approach with supporting materials

Cycle 1’s education campaign (section 8.5) was deemed more effective than Cycle 0’s campaign (section 7.5). Based on the positive impact of the campaign’s inclusion of pedagogical principles and provision of educational resources, Cycle 2 aimed to confirm the findings of Cycle 1 and further establish a more formalised education approach with supporting materials which are pedagogically sound by meeting the following two objectives:

1. **Cycle 2 – Objective 1 (C2O1): Provide further formalised, pedagogically sound educational resources.**

   Cycle 1 provided a small collection of pedagogically sound education resources for learners in the target group. This material had an impact on the learners. Most of them internalised the material’s content to some degree. C2O1 aimed to replicate and improve Cycle 1’s results by providing additional resources.

2. **Cycle 2 – Objective 2 (C2O2): Enable a further formalised education process by increasing the role of the expert educators (the teachers) in the educational component of the SACSAA campaign.**

   Lessons learnt in the Cycle 1 campaign showed that obtaining principal and teacher commitment to participation and subscription to the campaign and its messages contributes to the implementation and support of the campaign at the school (section 8.6, Lesson 9); and: using existing resources and experts should be encouraged where possible (section 8.6, Lesson 11). As part of the previous results, it was found that the participation and the level of internalisation was higher at schools where teachers had been more involved in encouraging participation and using the educational resources. Therefore, C2O2 aimed to encourage teachers to be more involved in the cybersecurity education process at their schools. This would align with both learnt lessons.
Addressing both objectives discussed above, Cycle 2 built upon the previous campaign cycles’ successes and lessons learnt.

9.2.2 Examine the effect of method(s) used to gain achieve school participation and gain the learners attention

Cycle 1’s actions taken to meet this issue had a noticeable effect on the participation rates in the campaign and competition. The advertising and personalisation and official interactions with schools to invite participation resulted in an increased number of schools opting to take part, and high numbers of learner participants. This resulted in Lesson 8 and Lesson 9 being learnt (section 8.6)

Most learners who depicted brand symbols on their posters related them to the cybersecurity or cybersafety messages included on their posters. The brand symbols were noticed by a portion of the target audience. The schools who had been exposed to direct introductions to the branding, where the symbols were discussed, had higher inclusion rates than schools where there were no formal introductions. This resulted in Lesson 10 being learned (section 8.6).

Cycle 2 implemented most of the iterations’ marketing and branding practices. However, it also investigated the issues of interest stemming from Lesson 10 (section 8.6). Lesson 10 found that the way in which brand symbols were used (introduced, highlighted, placed) in the resources affected their recognition and memorability for the learners. Cycle 2 aimed to further test the validity of Lesson 10 by examining other aspects of the inclusion of brand symbols.

Cycle 2 – Objective 3 (C2O3) is to: “examine whether the choice of brand symbol included in the education campaign affects the adoption of brand symbols”. A sub-objective would be to “consider the impact of the selected brand symbols on the formation of a SACSAA campaign brand identity and memorability” (C2O3A). This objective could also relate to whether specific sub-groups within a target audience have specific brand symbols preferences.

A further objective related to attracting learner participation and attention concerns the prizes offered as part of the poster competition. Cycle1’s campaign had valuable prizes advertised as motivation for participating in the competition. Feedback from the participants’ teachers indicated that the prizes were perceived by learners as incentives. An issue of interest raised because of this perception and the value of the prizes was whether the value of the prize affected the number
of entrants. Therefore, Cycle 2 – Objective 4 (C2O4) is to: “investigate whether the value of prizes affects the level of learner participation in the competition”.

9.2.3 Re-evaluate the effectiveness of the cybersecurity education game

Cycle 1 introduced the use of a BCE pedagogically sound game, the cybersecurity “Snakes, and Ladders”, as an educational tool. The educational effectiveness of this game was evaluated using the procedure outlined in Appendix E with a class of learners from School A (section 8.4.1.1). The results indicated that playing the game was effective in teaching learners about specific cybersecurity content.

The results of the evaluation were presented at the 2013 Kaspersky Student Conference. Feedback received highlighted the need to confirm previous findings on the game’s effect.

Cycle 2 – Objective 5 (C2O5) was to: “re-evaluate the educational cybersecurity game to determine its effectiveness in teaching learners from different target audiences and contexts”.

9.2.4 Increase the relevance and relatability of the campaign and its content for the learners

In Cycle 1’s campaign, implementation of some of the BCE principles made the teaching material engaging by personalising and contextualising the content for the learners. This was primarily achieved in the expert presentation component of the campaign. In Cycle 1, School A was the only school exposed to an expert presentation.

It was noted that those posters from School A which were fully internalised were considerably more contextualised in their depictions of the explanations of the cybersecurity concepts than those from the other schools (section 8.6). It was theorised that this result correlated with the learners having been exposed to the more contextualised and customised expert presentation and not simply the generic educational resources. Many information security education guidelines recommend designing efforts to suit user’s needs (Bishop, 2000; Bryce & Klang, 2009; NIST 800-12, 2004). Therefore, an issue of interest for Cycle 2 was whether highly contextualised and customised material would consistently result in learners developing and depicting a more personally contextualised understanding of the campaign messages.
Cycle 2 – Objective 6 (C2O6) was to: “design and implement the campaign and its content in such a way that it is contextualised and customised to the target audience”. The intent of C2O6 was to make the material more relevant and by extension easier for learners to relate to.

9.2.5 Determine whether a correlation exists between campaign’s content emphasis and the content choices learners depict in posters

The final issue of interest for Cycle 2 relates to the content included in the campaign as opposed to the content depicted by learners in their poster entries. The campaign aims to teach the learners about all cybersecurity issues that may affect them. The cybersecurity or cybersafety messages for each topic were all equally covered by the campaign’s educational material and expert presentations. However, the adoption rate of messages per topic was not equal. Definite trends in topic preference emerged, e.g. cyberbullying was a common message, while anti-piracy messages were not used in any posters. Both topics were relevant to the young target audience therefore this difference in use of the messages which were delivered in a similar manner was of interest to researchers.

The issue of interest for this cycle was therefore to determine whether placing greater emphasis on the topics which learners showed less inclination to adopt, as well as on the most prominent or adopted topics would affect the messages adoption rate. In brief, would campaign emphasis on particular topics result in a similar depiction rate of these topics among the learners?

Cycle 2 – Objective 7 (C2O7) was to: “investigate whether the amount of coverage particular content received within the campaign aligns with the degree to which the learners depict the topics in their posters”.

This section discussed the problem identification in Cycle 2 of the action research process. The next section presents the plan of action for studying and addressing Cycle 2’s problems.

9.3 Action planning

This section outlines the planned implementation for Cycle 2’s cybersecurity and safety awareness campaign and competition as it was intended to be implemented. Figure 9.1 presents
the section outline. The following section describes how implemented of the full campaign was planned for Cycle 2.

Figure 9:1 Cycle 2 action planning section outline

### 9.3.1 Target audience

In Cycle 2, the campaign’s target audience remained unchanged from 2012. The SACSAA campaign continued to target learners at both primary and high schools in the Nelson Mandela Metropolitan Area.

Many schools were invited to participate in the campaign. Six elected to participate in the educational campaign and to compete in the poster competition. The number of participating primary schools increased from one to four, while the number of high schools remained at two although one of these was included for the first time. The needs of the primary school audience were thus an important consideration in the design and presentation of this year’s educational resources.

School A and School AA participated for three second consecutive campaign cycles. Primary schools B, C, and D, and high school CC participated for the first time in Cycle 2.

Section 9.4 outlines the implementation of the campaign at these schools. Section 9.5 discusses the campaign’s results at each of these schools.
9.3.2 The Educational Campaign

Cycle 2’s campaign was designed and implemented to follow Cycle 1’s campaign procedure to a great extent. This included having separate, multifaceted educational campaign components.

The educational campaign followed a more formalised format, however, and was designed along brain compatible (BCE) principles outlined in Table 6.2. Cycle 2 continued to refer to the brain-compatible principles numerically as they are listed in Table 6.2. For each awareness resource, the relevant BCE principle/s are listed in their descriptions.

Taking into consideration the issues of interest of this campaign cycle, as outlined in section 9.2, this section outlines the components of the educational campaign. Additions and alterations to the campaign components included:

- Awareness-raising materials (section 9.3.2.1)
- expert presentations (section 9.3.2.2)
- branding (section 9.3.2.3)
- invitation (section 9.3.2.4)

The following sections discuss these measurements.

9.3.2.1 Awareness-Raising Materials

As part of the formalisation of the cybersecurity education campaign, the C2Ol was to “provide further formalised, pedagogically-compliant educational resources”. The planned awareness-raising materials for inclusion as part of the campaign therefore included the awareness materials from Cycle 1 and additional awareness materials.

The resources from the previous cycles, which were to be reused in Cycle 2, included:

- the original topic-specific flyers with single security messages (Figure 8.2, section 8.3.2.1.1)
- the cybersecurity snakes and ladders board games (Figure 8.3, section 8.3.2.1.2)
- and the cybersafety pledge and Cyber Sid (Figure 8.4, section 8.3.2.1.3)
- the cybersafety 101 flyer (Figure 8.5, section 8.3.2.1.4)
New materials were:

- additional 101 flyers with separate 101 topics (Figure 9.2, section 9.3.2.1.1)
- the NMMU SACSAA calendar (Figure 9.3, section 9.3.2.1.2)

Expert presentations would also continue to be offered. The expert’s educational lecture was somewhat altered, with a refinement of the presentation and content from Cycle 1’s implementation. The branding was also investigated. Each of the new and altered materials and campaign components are briefly described below.

### 9.3.2.1.1 Additional 101 flyers

Four more 101 flyers were added to the material (Figure 9.2). Flyers covered the topics of Public Wi-Fi Safety, Facebook Security, Internet Banking, and Parental Control. The posters were designed and created to follow the same BCE principles, format, and layout as the first Cybersafety 101 awareness flyer (section 8.3.2.1.4). It was hope that the inclusion of separate topic flyers would place emphasis on topics and encourage learners to take more notice of them. This practice would contribute to meeting C2O7.

![Figure 9:2 Additional 101 Subject-Specific Awareness-Raising Flyers](image-url)
Each of the 101 flyers provided in-depth advice on their specific issues in the format of seven “golden rules” for the particular cybersecurity issue. The educational rules outlined basic behaviours that users (learners) should and should not adopt. Relevant and straightforward examples and explanations were provided for each rule in each flyer.

As discussed with regard to the first cybersafety 101 flyer, the BCE principles applicable to these resources were BCE Principles 1,3,5 and 6 (section 8.3.2.1.4).

9.3.2.1.2 Calendar featuring pictures of previous years’ winning posters

In Cycle 1, a motivator for participation was the use of the competition winners’ posters in a calendar and other SACSAA awareness-raising materials. Feedback from the teachers indicated that learners, particularly those at primary school, regarded this a definite incentive to participate. In Cycle 2, the first awareness calendar for the campaign was printed, using Cycle 1’s winning posters (figure 9.3).

Apart from being used to encourage participation, the calendar is also an educational resource. It is an awareness-raising resource designed to appeal to and relate to learners.

Figure 9:3 2013 SACSAA Cybersecurity calendar with past winners’ posters
The calendar was designed as an annual flip calendar. Figure 9.3 provides an example of the two pages of the calendar for December. Each month included a winning poster, and a cybersecurity tip for the user which related to the topic area/s included in that month’s poster. Calendars were distributed to winners and to the schools that took part in Cycle 1, and they were included in the Cycle 2 invitation packs.

As a result of their media-rich nature, it could be argued that the calendars themselves are educational resources grounded in BCE principles. However, their primary purpose in the campaign was to motivate future participants and to reward past participants.

9.3.2.2 Expert presentations

Schools were to be given the option of being visited by a SACSAA representative who would deliver an educational presentation. This presentation was a recommended but voluntary part of the campaign. Expert presentations aimed to meet C2O1.

The title of the presentation to be delivered by an expert in Cycle 2 was “Cybersecurity Self-defence v.2”. Most of the campaign’s design and implementation details, and its BCE principles were repeated from the expert presentation used in Cycle1 (section 8.3.2.2). However, a new presentation was created, which took into consideration the lessons learned in Cycle 1 as well as Cycle 2’s objectives.

The first difference was the degree to which each topic was emphasised. In order to meet C2O6, and in keeping with BCE principles 3 and 5, the expert presentation aimed to customise and contextualise the presentation’s topic emphasis and examples, based on their relevance to the needs of each school. This tailoring of the material made the presentation it more engaging and relevant and therefore easier to learn and draw parallels from (BCE principles 1, 3 and 4).

Each school’s teacher(s) would be asked to specify the topic(s) which they believed were most relevant to the problems their learners faced. Greater emphasis was placed on the teacher’s highlighted topics and also on those topics that had been neglected in Cycle 1, e.g. piracy. As a result, each school received versions of the talk tailored to make the content relevant to those learners’ context and experiences. Presentations could even be tailored to different age-groups (grades) in order to focus on age-appropriate activities and associated cyber dangers.
It was hypothesised that the resulting variances in topic emphasis would also assist in meeting C2O7. The researcher would be able to identify which topics were emphasised in the talk at each school and compare these with the topics the school’s learners chose to include in their posters.

The second difference in the presentation was that the SACSA logo was the only brand symbol included in this year’s presentation; the Cyber Sid mascot was excluded. This design decision relates C2O3 and C2O3A and will be discussed in the next point.

The third difference was that where possible Cycle 1’s winning posters were included as examples of relevant topics. This made the material more relevant, media-rich, provided reinforcement of concepts and attracted learners’ attention (BCE principles 1, 3 and 7). It also aimed to motivate learners to take part and possible be featured in future resources.

The fourth difference was an increased use of learners as active participants in the presentations. Learners could volunteer to take part in demonstrations (acting out concepts) of concepts during the talk. It was hoped that this would increase interactivity, engage the audience, and make the demonstration more fun (BCE principles 1, 2 and 7). The Q&A session was retained, and used more often during the presentation (BCE principle 6).

9.3.2.3 Branding

Cycle 2 continued to use brand symbols to make the material relevant and memorable for the learners. This plan to continue using branding was intended to encourage a brand identity for the SACSA campaign and encourage associations in learners through a strong logo message (visual-verbal). This would be in keeping with the implementation of BCE principles 3 and 5. The frequent inclusion of the brand symbols would assist in creating appropriate associations and provide learners with multiple opportunities to see the brand symbols included alongside cybersecurity or cybersafety messages (BCE principle 6).

Cycle 1’s results showed moderate adoption of the Cyber Sid mascot (figure 8.7, section 8.3.2.3) and limited adoption of the SACSA logo (figure 8.6, section 8.3.2.3) in learner posters. Cycle 1 included the brand symbols in the awareness-raising materials and the expert presentation, and their backgrounds and stories were explained during expert presentations. School A was the only school to receive explanatory introductions to the brand symbols, and the only school where learners included the brand symbols. It was therefore inferred that the way branding was introduced mattered, and that actively introducing learners to the branding encouraged its
adoption. Cyber Sid had been more thoroughly introduced than the SACSAA logo and had a correspondingly higher adoption (depiction) rate. Lesson 10 was extrapolated from this finding.

In order to further explore lesson 10’s validity, C2O3 and sub-objective C2O3A were outlined. In order to examine these objectives, it was decided that the brand symbols would be introduced separately in different cycles of the campaign. They would be directly introduced, and used in the same way as far as possible. Their adoption rates would then be compared. C2O3 and sub-objective C2O3A would therefore be examined in stages. The preceding Cycle 1 began this, it was explored in Cycle 2 and would be followed by further examination in Cycle 3.

Cycle 1’s results revealed that Cyber Sid had a higher adoption rate. It was decided that Cycle 2 would examine the use of the SACSAA logo as the primary brand symbol. The SACSAA logo replaced the Cyber Sid mascot on all the educational material and awareness-raising resources provided to schools. In addition, the SACSAA logo was featured prominently in the expert’s presentation material and lectures. The logo was also prominent in Cycle 2’s invitation and competition advertisement (Appendix D Figure 2).

9.3.2.4 Invitation to participate

Cycle 1 began the campaign early in the year. This was done to allow schools and teachers time to encourage students to take part, and/or to incorporate material into their classes or place it in visible areas within the school. The earlier start date led to levels of participation increasing significantly in 2012.

The plan for Cycle 2 was to continue Cycle 1’s launching of the campaign early in the year. The due date of the competition remained the last week of October (SACSAA Cybersecurity and Safety Awareness Week). The plan to advertise and encourage participation built on Cycle 1’s implementation. Invitations and resource packs were sent to the schools in the metropole via post and via e-mail at the very beginning of the campaign. The packs contained:

- a professionally designed advertisement (Appendix D Figure 2)
- the awareness-raising materials (topic-specific awareness flyers (Figure 8.2, section 8.3.2.1.1), “Snakes and Ladders” cybersecurity game (Figure 8.3, section 8.3.2.1.2), cybersafety pledge forms (Figure 8.4, section 8.3.2.1.3), the cybersafety 101 flyer (Figure 8.5, section 8.3.2.1.4), the additional 101 flyers (Figure 9.2, section 9.3.2.1.1), and the SACSAA calendar featuring previous years’ winning posters (Figure 9.3, section 9.3.2.1.2)
- a request form (and contact details) for a free expert presentation
• a cover letter explaining the importance of cybersecurity and the campaign and why it was relevant to children, and what participation would entail.

Plans were made to visit the schools in person to speak to the principal or school teachers who would be involved in championing the campaign at the school. This decision was in keeping with BCE principles 2 and BCE 5. This visit would involve face-to-face interaction and the establishment of trust in the campaign. It was also an opportunity to explain the campaign’s importance in relation to establishing a societal cybersecurity culture starting with learners, schools and the larger SACSAA campaign. If the schools had not received an invitation package via the post or e-mail the researchers provided one upon their visit.

In order to meet C2O2 they were asked, firstly, to incorporate the resources into at least one of their own lessons to reinforce the researcher’s guest lectures. Secondly, they were asked to encourage their learners to take part in the campaign. It was not compulsory for the schools to comply with these requests; however, the researcher did indicate that it was the recommended course of action.

The requests were included as part of the cover letter explaining what participation entailed, and the campaign representative explained the requests during visits to the schools.

### 9.3.3 The Competition

Invitations to take part in the poster competition were included in the educational campaign’s information and resource packages. The overall purpose of the competition did not differ from that of Cycle 1. The competition was partially educational but also the method by which data were gathered about the campaign’s impact on learners.

The competition had two components: posters and prizes. Implementation of the competition in Cycle 2 made only minor changes to Cycle 1’s procedures. These changes are outlined in the description of components.

• **What to enter**

Based on the success of Cycle 1’s data collection, the competition issued a call for poster entries for the competition. Thus, the data gathering tool remained unchanged. However, to address some of the queries received in Cycle 1’s campaign, some design rules were provided.
The first rule was that learners could submit only one entry, which as to be their own individual work. This rule aimed to ensure that the participation measurement was a true reflection of the number of learners involved. This rule had previously been unofficially implemented.

The second rule was that learners could create posters depicting one or more cybersecurity and/or safety topics. This was intended to allow the measurement of those topics to which learners truly related. They were required to depict the topic(s) as if they were trying to raise cybersecurity and/or -safety awareness amongst their peers.

The third rule constituted a set of guidelines for formatting the poster entries. The posters could be hand-drawn or digitally created. All images and text was to be a learner's own original work. Copyright infringements would be disqualified. The posters could be on A4 or A3 sized paper.

- **Prizes**

C2O4 aimed to investigate whether the value of prizes affected the level of participation. Cycle 1 had offered and advertised very generous prizes for competition winners. Teachers had indicated that their learners considered the prizes a factor that contributed to motivating them to participate in the competition.

As in Cycle 1, generous prizes were offered to motivate learners to take part. However, the value of the prizes was lower than those of Cycle 1. The value was reduced to determine whether the value of the prize significantly affected the levels of participation; would there be a relationship between lower prize value and participation levels? Prizes were advertised for the "Top 15" entrants.

Cycle 1 had offered a prize for the school with the most participants in an attempt to motivate teachers to encourage participation. However, feedback from teachers indicated that this prize was not a major motivation. Most teachers indicated that they had not been aware of the prize even though it was advertised. No school prize was offered in Cycle 2.

Winning posters would be incorporated into future SACSAA campaign educational materials. Such materials included an awareness-raising calendar, which was hoped would be distributed to campaign supporters and participants. The potential inclusion of their work in the resources served as an additional motivation for the participants to enter the competition.
Chapter 9 Cycle 2: 2013

9.3.4 Measurements for use in the analysis of the campaign

The success of Cycle 2’s campaign was evaluated using the data gathered from the poster competition. A qualitative content analysis, as described by Krippendorff (2004), was used to analyse entries. In the analysis, the following questions were asked:

1. How many learners participated? (section 9.3.4.1)
2. What topic(s) is covered by the message(s) in the poster? (section 9.3.4.2)
3. How well has the cybersafety message been internalised (in the researcher’s opinion)? (section 9.3.4.3)
4. Which brand symbols, if any, are present in the posters? (section 9.3.4.4)

These four measurements were used to establish the overall effectiveness of the cybersecurity and safety education campaign. In Cycle 2, as in Cycle 1, a separate analysis was conducted to measure the effectiveness of an educational cybersecurity game that was designed to be pedagogically sound (section 9.3.4.5). The repetition of this measurement in different context(s) was intended to confirm or disprove the findings of Cycle 1’s evaluation of the game.

The primary reasons for the measurements and methods of gathering the measurements remained unchanged from Cycle 1 (section 8.3.4). However, some additional reasons are briefly described below.

9.3.4.1 Learner participation

In Cycle 2 this metric measured whether the number of participants each year was influenced by:

- **Contextualisation of the material**
  Cycle 2 contextualised the expert’s presentation and relevant material to focus on specific issues faced by learners at each school. This customisation of the presentation may have resulted in the learners being more engaged and interested in the campaign, resulting in them taking part in the competition.

- **Teachers’ encouragement and involvement**
  Teachers were asked to take a more active role in the education process. They were asked to use the educational materials in at least one classroom lesson and to regularly encourage learners to take part in the campaign and competition.

- **The value of the prizes**
  The value of the competition’s prizes was lower than in Cycle 1.
9.3.4.2 Posters per topic

This measurement would assist in evaluating whether the topics which learners depicted in their posters corresponded with the topics emphasised in the campaign. This would be particularly measurable at schools which had allowed customised expert presentations.

9.3.4.3 Internalisation of Cybersecurity or Cybersafety Message

This measurement aimed to determine whether Cycle 2’s provision of additional educational resources, together with the customisation and contextualisation of the expert presentations had contributed to increasing the percentage of learners who internalised the material to some degree. Material customisation, and in some cases repeated exposure to material, could result in a corresponding increase in internalisation of the cybersecurity or cybersafety messages by learners. At schools where teachers had complied with the request to incorporate the educational materials into at least one of their lessons, this measurement could also indicate whether increased teacher involvement improves message internalisation.

9.3.4.4 Presence of Brand Symbols

The purpose of this measurement was unchanged; however, in Cycle 2 the focus was primarily on the presence of the SACSAA logo in the poster submissions.

Based on this planned implementation of the branding, the measurement would show whether as Cycle 2’s sole brand symbol, the SACSAA logo appealed to learners, or to particular learners. This could then be compared to the results of Cycle 1’s higher rate of adoption of Cyber Sid than of the logo, and Cycle 3’s planned mascot inclusion measurement.

School A was the only school that had had a direct introduction to both the mascot (in Cycle 1) and the logo (Cycle 1 & 2). This school’s results could indicate whether Cycle 1’s branding had been memorable. For example, if Cyber Sid were to be depicted despite not being included in this year’s material, this would suggest that it was a memorable brand symbol.

9.3.4.5 Evaluation of pedagogically sound cybersecurity education game

In Cycle 1, the pedagogically designed board game “Snakes and Ladder” was introduced as a cybersecurity education tool. Its effectiveness as an educational tool was evaluated using a series
of assessments that tested learners’ knowledge before, immediately after, and some time after playing the game. Informal discussions were also held with teachers after the final assessments, to measure their perceptions of the game and its effect on learners’ knowledge and behaviour.

School A participated in Cycle 1’s evaluation of the game. The results of the assessment and the teacher’s perception indicated that the game was effective as an educational tool (section 8.5.1.6). The results of the case study were presented at a student conference. Feedback received from participants and experts recommended further implementations of the evaluation in different cases to determine whether the game was consistently successful in educating learners about cybersecurity.

In this campaign cycle, the effectiveness of the game was re-evaluated using the same procedure as in Cycle 1 in different cases (section 8.4.1.1). The game was evaluated based on:

- the game’s impact on learners’ knowledge of password security management
- teachers’ perceptions of the game’s effect on learners’ knowledge and behaviour.

The implementation of the evaluations is discussed in section 9.4.2.1.1.

Section 9.3 outlined the recommended campaign implementation for the Cycle 2 iteration. The next section describes the actual implementation of the campaign iteration.

**9.4 Implementation**

This section describes how the campaign was implemented at each school that participated and submitted posters. Implementation was dependent on what the school would allow and support. In Cycle 2, the school’s implementation and results were discussed in relation to their implementation choices. Schools that made the same implementation choices were grouped together. This was done to simplify discussion and comparison of the results of schools with similar and different implementation experiences.

School A continued to follow the recommended implementation of the campaign and is discussed first as constitutes a group on its own (section 9.4.1). The implementation at the remaining participant schools is discussed in the following implementation categories:

- Recommended implementation (section 9.4.2.1)
- Teacher-oriented implementation (section 9.4.2.2)
- Limited implementation (section 9.4.2.3)
The campaign’s implementations at each school are briefly described below.

9.4.1 School A

The school was asked to participate via postal and personal invitation. The latter was delivered in a meeting between the SACSAA representative, the principal and the teachers who would be involved in implementing the campaign at the school. The school chose to follow the recommended version of the campaign. The school therefore:

- accepted the materials
- agreed to have an expert address their learners in a guest lecture
- committed to teachers using the materials in at least one lesson of their own
- committed to regularly encouraging learners to participate in the campaign and competition

Two versions of the expert presentation were presented at the school to two grade groups. The examples, discussions, and other customised features of the presentations were adjusted to suit each group. Teachers requested that the customised presentation focus on the issues of cyberbullying, personal information disclosure, and viruses and malware. They asked that all three of the topics be emphasised with the senior primary learners. Cyberbullying and personal information disclosure were focused on in the junior primary presentation.

9.4.2 Other Schools

Three groups of implementation patterns emerged from these schools. These are briefly described below.

9.4.2.1 Recommended implementation

School B and School D were both first time participants. Both schools received a postal invitation and a visit from a SACSAA representative. The initial meetings involved the SACSAA representative, the principal and the teachers who would be involved in the campaign activities at the school.

Both schools chose to implement the recommended implementation of the campaign in the same manner as School A. There were some minor differences in the expert presentation at the two schools. Both schools decided on cyberbullying as a topic of focus. Cyberbullying was considered
an important issue by both schools. At School B, teachers requested that personal information protection (information and password security) be the focus as this was an issue they believed to affect all their learners.

School B’s teacher exposed the whole school to the campaign. Ages of participants therefore ranged between six and 13 years of age. On the other hand, School D focused on Grade 4 learners only, whose ages ranged from nine to 11.

**9.4.2.1.1 Evaluation of pedagogically designed cybersecurity education game**

To meet C2O5, School B and School D participated in the re-evaluation of the educational “Snakes and Ladders” cybersecurity game. The evaluation was implemented using the same procedures and tools as in Cycle 1’s study at School A (section 8.4.1.1, Appendix E).

In the evaluation of the game, the participating class from School B consisted of nine Grade 3 learners between the ages of 9 and 11 years. The participant class from School D consisted of 15 Grade 5 learners between the ages of 12 and 14. The results of this evaluation are presented in Section 9.5.2.5.3.

**9.4.2.2 Teacher-oriented implementation**

This was the second year of participation for School AA, and the first for School CC. It should be noted, however, that the learners from School AA were not the same learners as those who had participated in Cycle 1, as they had been in grade 10 in 2012. Therefore, neither group of learners had been previously exposed to the campaign materials.

Both schools received a postal invitation and a visit from a SACSAA representative. The initial meetings involved the SACSAA representative, the principal and the teachers who would be involved in the campaign activities at the school.

School AA and School CC both opted to follow the recommended campaign procedure but excluded the expert presentation from the programme. This approach relied primarily on the active championing of the material by teachers.

The teachers displayed and used the material in their lessons. School AA made use of the material in multiple information technology and life orientation classes with cybersafety and -security themes. The teachers at School AA presented an estimated four lessons using the material to all the Grade 11 classes. School CC provided feedback that the teacher had made
use of the material in two lessons dedicated to online safety and security in each of their Grade 8 classes. The teacher at School CC indicated that emphasis had been placed on the topic of cyberbullying, an issue which had recently been faced by some of the learners at the school.

School AA learners who participated in the competition were aged between 16 and 18 years of age. School CC’s learners were aged between 13 and 15 years.

**9.4.2.3 Limited implementation**

School C was a first-time participant. The school received a postal invitation and a visit from a SACSAA representative. The first meeting involved the representative and the principal; no teachers were in attendance. The school decided to participate but did not want an expert presentation to be delivered to learners.

The school reported that it had implemented the campaign by placing the materials and the competition advertisement on a general noticeboard in the hall. This school’s implementation of the campaign was most like Cycle 0’s implementation, but with more educational materials. Learners had to educate themselves. Participation was self-motivated.

**9.4.2.4 Competition Judging**

Reminders of the competition’s closing date (final submission) were sent out via e-mail to all the schools who had been invited to participate. The reminders also confirmed the date by which schools would be notified of the winners, and the date of the prize giving.

Section 9.4 provided the real-world implementation details of the 2013 SACSAA campaign and poster competition at each participating school. The following section presents the results of the campaign and competition at School B and School D as well as the results of the evaluation of the cybersecurity game.

**9.5 Results and Evaluation**

This section presents the results of the 2013 SACSAA Educational Campaign and competition. The layout of the chapter is presented in Figure 9.4. The section begins by examining the results of School A, and is followed by a discussion of the results of the other schools in Cycle 2’s
The section concludes with a discussion of the results of the campaign as a whole from the analysis of data from all participants.

Some of the results presented in this section have been published. Where relevant, the publication(s) will be acknowledged. Some differences exist between the published data and the data presented in this section. The data included in this section are the most complete and correct data, including some sources that were not available at the time of the publications.

**9.5.1 School A**

This section presents the findings from School A. Measurements from Cycle 2 include: the number of participants from the school, the number of posters depicting each cybersecurity or -safety topic, the degree to which the cybersecurity or cybersafety messages were internalised and finally, the number of posters that included the campaign mascot or other brand symbols (brand identifiers). Each of these measurements are discussed below. The results from this school and cycle were published in (Reid & Van Niekerk, 2014c), (Reid & Van Niekerk, 2015) and (Reid & Niekerk, 2016).
9.5.1.1 Learner participation

School A showed a decrease in number of poster entries in Cycle 2. In Cycle 1, most of the learners (94) had participated in the campaign and competition. In Cycle 2, approximately half the school population had participated in Cycle 1 (57 learners).

This decrease occurred despite the changes to the campaign which were aimed to improve its results. A reason for this drop in participation could not be identified until feedback was received from teachers after the competition closed. The teachers had identified potential winners from their learners’ submissions. This was the reason for the decrease in entries. Those entries discarded by teachers had been recycled and were not available for analysis.

As a result of this preselection of posters an accurate measurement of the impact of the contextualisation of the material, increased teacher involvement or decreased value of the prizes on the participation of the learners in the competition could not be established. However, feedback from teachers indicated that most of the school’s learners had created a poster before the preselection; it can thus be posited that the actions had a positive impact. The feedback also indicated that the prizes, despite their lower monetary value than those in Cycle 1, and the possibility of having their work included in future resources remained a motivation for students to participate in the competition.

9.5.1.2 Posters per topic

The campaign covered many topics in its resources (section 9.3.2). The main difference between the campaign content to which each learner was exposed came from the optional expert presentations. C2O6 and C2O7 led to the customisation of the campaign, and the different levels of emphasis placed on particular cybersecurity topics at each school.

School A requested that special emphasis be placed on the topics of cyberbullying, viruses and malware and personal information disclosure. Whether there was a correspondingly equal representation of these topics in the learner's submissions was an issue of interest relating to C2O7. Figure 9.5 presents the percentage of Cycle 2 posters that covered each topic. It also provides a comparison to the topic coverage percentage of Cycle 1’s submissions.
Figure 9.5 Percentage of School A’s competition posters per topic: Cycle 1 to Cycle 2
The analysis of School A’s poster submission in Cycle 2 found that in comparison to Cycle 1, there was an increase in the percentage of posters including the topics of:

- cyberbullying – 26% (Cycle 1) to 32% (Cycle 2)
- information and password security – 49% (Cycle 1) to 53% (Cycle 2)
- viruses and malware – 49% (Cycle 1) to 53% (Cycle 2)
- social networking – 15% (Cycle 1) to 18% (Cycle 2)
- piracy – 0% (Cycle 1) to 2% (Cycle 2)
- Browsing and downloading – 5% (Cycle 1) to 7% (Cycle 2)
- dangers of online activities – 11% (Cycle 1) to 14% (Cycle 2)

The first three topics had been earmarked by the school for emphasis. Social networking related strongly to the cyberbullying and information disclosure messages. Piracy was a topic on which the expert had placed considerable emphasis based on the lack of message adoption in Cycle 1. Browsing and downloading and the dangers of online activities were topics that both related strongly to all the emphasised topics.

There was an increase of posters submitted for topics that were emphasised during campaign presentations. This may have occurred because students now deemed these topics more relevant to their own context, or because they regarded them as particularly relevant to the competition. Either way, the researcher believes that there was an increased awareness of these topics.

The only significant drop in topic coverage by learners was in the category of stranger danger. The percentage of posters focused on this topic decreased from 40% (38 of 94) to 30% (17 of 57). The focus on this topic was closely related to non-disclosure of personal information, particularly for younger learners. The topic had been strongly emphasised to the junior primary learners, more so than senior primary learners in Cycle 1. This had been possible owing to the separate assemblies. In Cycle 1 and Cycle 2 most of the posters that had included stranger danger messages were submitted by younger (junior primary) learners. The number of posters received from junior primary learners in Cycle 2 was lower than in Cycle 1. This might be attributable to teachers pre-selecting and not submitting all created posters

### 9.5.1.3 Internalisation of Cybersecurity or Cybersafety Message

This measurement showed the degree to which learners had internalised the cybersecurity or cybersafety messages which they had illustrated in their posters. Figure 9.6 reflects the percentage of posters per internalisation level.
School A’s poster analysis showed that an 81% (47 of 57) majority of the learners had to some degree internalised the cybersecurity or cybersafety message. A 18% (10 of 57) minority had not internalised the cybersecurity or cybersafety messages.

In terms of percentages, this was a significant increase in learners who did not internalise the message. However, numerically this represented an increase of only three students. The difference in the percentages is attributable to the overall number of posters submitted. A true measurement of the level of internalisation could not be fully achieved for School A because analysis could not be conducted on posters that teachers had decided not to submit.

Based on the data, the percentage of learners in each internalisation position had decreased. In addition, the distribution of the other internalised posters between levels was the same as in Cycle 1. This may indicate that, had the data received been complete, they would have equalled or improved upon Cycle’s results.

Based on School A’s data, the actions taken to meet C2O2 resulted in learners being educated. Additional pedagogically sound materials and an increased involvement of expert educators had a positive impact on the degree to which learners had internalised the taught cybersecurity or cybersafety messages. In addition, the customisation and contextualisation of the materials, in
keeping with C2O6, also led to an increase in the number of learners who fully internalised the messages.

An interesting trend was that the topics which were particularly emphasised in the expert presentations were fully internalised or rephrased by a greater number of learners.

### 9.5.1.4 Presence of Brand Symbols

This measurement quantified the adoption of the campaign’s brand symbols. Cycle 2 focused on actively introducing the SACSAA logo as a prominent campaign brand symbol. The logo was directly introduced during expert presentations, included in all the educational resources, and included on all official communications and advertisements. School A was exposed to this promotion. It was also the only school to be exposed to a similarly direct promotion of the Cyber Sid mascot in Cycle 1. Figure 9.7 shows the percentage of learners who used either or both the brand symbols in Cycle 2.

![Figure 9.7 Percentage of School A’s posters depicting brand symbols: Cycle 1 to Cycle 2](image)

<table>
<thead>
<tr>
<th>Brand Symbol</th>
<th>Cycle 1</th>
<th>Cycle 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Sid Mascot</td>
<td>20</td>
<td>21</td>
</tr>
<tr>
<td>SACSAA Logo</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>All Branding Symbols</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>No Branding Symbols</td>
<td>69</td>
<td>72</td>
</tr>
</tbody>
</table>

Most School A learners did not include a brand symbol in their posters. There was also a slight decrease in how many learners included the brand symbols, although a percentage of the learners depicted all brand symbols.
The percentage of learners who included both brand symbols increased from 1% (1 of 94) to 4% (2 of 57). The percentage of posters depicting the Cyber Sid mascot increased from Cycle 1 (20%, 19 of 94) to Cycle 2 (21%, 12 of 57). This indicates that the mascot was noticed by learners who had previously been introduced to it as a brand symbol. Conversely, the percentage of learners who included the logo decreased from 10% (9 of 94) to 4% (2 of 57). This may be related to the possible exclusion of posters which had contained the logo. Alternatively, it could indicate that these learners did not relate to or adopt the SACSAA logo as a brand symbol with which they could associate the cybersecurity or cybersafety messages.

In relation to C2O3, at School A the direct introduction of the Cyber Sid mascot in Cycle 1 appeared to have made it more relevant to learners than Cycle 2’s use of the SACSAA logo. Similarly, in this cycle, the mascot was more memorable than the SACSAA logo, which had been promoted in Cycle 2.

This section presented the results from Cycle 2 of the action research process for School A’s data. The next section presents this research cycle’s campaign’s results for the remainder of schools that participated in the 2013 SACSAA campaign.

9.5.2 Other Schools

This section presents the results of all participating schools except School A. Schools’ results are grouped according to their implementation details (section 9.4.2). For each measurement, each school’s results will be discussed as part of the implementation group. The results from this school and cycle were published in (Reid & Van Niekerk, 2014c).

9.5.2.1 Learner participation

This measurement assessed whether the changes made to the campaign had affected the number of learners who took part.

9.5.2.1.1 Recommended implementation

School B and School D were exposed to the campaign in its recommended implementation format. Thus, they were exposed to all the campaign’s resources and activities, and all the actions taken during Cycle 2 to make them as effective as possible. It was their first year of participation, so their participation rates cannot be compared to previous years’ measurements. At both
schools, most learners exposed by teachers to materials and lessons and whose participation had been actively encouraged took part in the poster competition. The number of submissions from each school is shown in Table 9.1.

### Table 9.1 Number of poster entries from other schools (recommended implementation): Cycle 2

<table>
<thead>
<tr>
<th>School</th>
<th>Cycle 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>School B</td>
<td>102</td>
</tr>
<tr>
<td>School D</td>
<td>70</td>
</tr>
</tbody>
</table>

Large groups of learners from School B and School D took part in the education campaign and the poster competition. For School B, this comprised most learners attending the school; for School A, this represented most of the learners in Grade 4. School B’s submissions included 71 hand-drawn entries and 31 digital posters. All School D’s entries were digitally created.

Feedback from the teacher involved at each school indicated that many learners did consider the prizes and the possibility of having their work featured in materials like the calendar as motivation to participate. This confirmed the need for prizes and *Lesson 12*. Prizes and recognition were not, however, the only motivators identified in the feedback.

The teachers highlighted the participation of learners’ peers, the entertaining aspects of the experience and their teachers’ enthusiasm and frequent reminders about the campaign and competition as other reasons learners gave for taking part. This feedback assisted in further validating *Lessons 9 and Lesson 11*.

In relation to *Lesson 9*, having the support of teachers positively affects the implementation of the campaign at schools, and by extension participation levels. In addition, involving the teachers as experts in the educational component of the campaign also contributed to increasing participation (*Lesson 11*). This may be further validated by the measurement of the learner’s internalisation of the content.

### 9.5.2.1.2 Teacher-oriented implementation

Table 9.2 shows the number of participants from each school who were exposed to the teacher-oriented implementation of the SACSA campaign in Cycle 2 as well as their previous cycles' measurements. The learners were exposed to all resources excluding the expert presentations. The schools’ teachers were the primary guides in using the educational resources as part of learners’ educational experiences. School AA had participated in Cycle 1; therefore, its previous
participation data was included in the figure for comparison. School CC had not taken part in Cycle 1.

Table 9.2 Number of poster entries from other schools (teacher-oriented implementation): Cycle 1 – Cycle 2

<table>
<thead>
<tr>
<th></th>
<th>School AA</th>
<th>School CC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle 1</td>
<td>122</td>
<td>0</td>
</tr>
<tr>
<td>Cycle 2</td>
<td>90</td>
<td>103</td>
</tr>
</tbody>
</table>

Both School AA (90 learners) and School CC (103 learners) had many participants. At each school, all the learners in the grades that teachers had selected for the campaign materials participated. School AA showed a decrease in the number of participants from Cycle 1; this was attributable to the different class sizes at the school. All the submissions from both schools were digitally created.

Feedback received from teachers indicated that use of the materials in the classroom had appealed to learners. They had worked through the materials provided with ease. The teachers said that, based on their discussions with learners, incentives for taking part in the competition included:

- advertised prizes
- shared social concern relating to the issue
- teacher’s frequent reminders about the competition and the class time in which they could work on their entries.

Overall, teacher involvement played an influential role in encouraging learners to pay attention to and learn from the educational resources. This resulted in their participation in the competition. School AA’s teacher indicated that future campaigns should provide additional, more advanced content resources for use in the classroom.

9.5.2.1.3 Limited implementation

School C only had two campaign and competition participants. This school barely implemented the campaign and its implementation confirmed the findings of Cycle 0’s campaign. Relying on learners to self-educate and self-motivate their participation is not effective with this age group.

Lesson 2 was reconfirmed. The attention of two learners was attracted by the campaign advertising but a more active approach involving experts, or a teacher may have been more
effective if other schools’ results are anything to go by. The attention of other learners may also have been attracted but they did not take part in the poster competition.

Based on feedback from the school principal, it appears that the prizes motivated learners who submitted posters to participate in the competition. This could indicate that the value of the prize did not significantly matter to learners provided there was a prize they could aim for (C2O2). This finding validated Lesson 12.

### 9.5.2.2 Posters per topic

The schools were exposed to different implementations of the campaign. Differences included:

- how learners were exposed to the provided resources
- whether they were exposed an expert presentation
- the different degrees to which the content was emphasised, based on teacher requests or actions
- The contextualisation and customisation of the expert presentation.

This measurement indicated the effect actions and experiences specific to each implementation had on learners’ ability to relate to, empathise with or recall taught lessons on the topic(s) depicted in their competition posters.

#### 9.5.2.2.1 Recommended implementation

Figure 9.8 shows the percentage of each school’s competition posters that depicted content from each topic. Both School B and School D showed a trend in depicting messages on the topics of information and password security, cyberbullying, and stranger danger. The order of frequency of topics did, however, differ in the two schools. School B’s most depicted topic was information and password security (43%, 44 of 102) followed by cyberbullying (38%, 39 of 102) and then stranger danger (28%, 29 of 102). On the other hand, most of School D’s posters focused on cyberbullying (64%, 43 of 70), while much fewer focused on information and password security (14%, 10 of 70), followed by stranger danger (13%, 9 of 70).

School B reflected greater adoption of the topic of stranger danger; this may be the result of participants including learners in the age group six to 13 years. Most of School B’s learners who used stranger danger messages were aged between six and eight years. This age group may
relate more strongly to this message because it is similar to other stranger danger messages they are often exposed to in their life orientation lessons.

In comparison, School D’s participants’ ages ranged from nine to 11 years. As a slightly older audience, they had begun to move beyond the basic dangers posed by strangers and had started to focus on peer-group pressures or dangers as well as the more abstract dangers of information disclosure. Their depictions of stranger danger typically related to warning against the disclosure of personal information or trusting phishing messages.

There was a relationship between the number of learners who depicted topics, and the level of emphasis that the materials, and especially the expert presentation, had placed on the topics in fulfilling teachers’ requests for customisation and contextualisation. School B had requested focus on cyberbullying and information security, and their posters depicted a strong adoption of messages from both topics. School D requested greater focus on cyberbullying, with special emphasis on examples and consequences of bullying. A particular adoption of the anti-cyberbullying messages was apparent. These findings suggested that messages to which learners related to would show a high adoption rate.

Overall, the findings from these schools reflected the same trends as School A in that emphasis in the expert presentation and support from the educational resources affected the adoption of messages. This emphasis was augmented by teachers’ use of the materials in lessons and their focus on topics they considered important. Feedback from teachers indicated that in using the educational resources in their own lessons, they had also tended to focus on the topics for which they had requested as special focus in the expert presentation.

These consistent findings are the start of a lesson that supports the issue of interest that the emphasis that materials, experts, and activities place on specific content can affect the adoption of this content by learners. This finding may relate to the customisation and contextualisation of the campaign content based on the campaign’s goals. This lesson is discussed in detail in section 9.6.5.

This possible lesson is not without exceptions, however. Learners from both schools showed a disinclination to depict messages for the topics of browsing and downloading, and piracy, with no learners depicted them in their posters. The educational materials, particularly the expert presentation, covered these topics in some detail, particularly piracy, however as in Cycle 1 learners did not adopt them. This suggests that even if every educational effort is made to address an issue, if learners do not relate to or support a lesson’s message they will not adopt it.
Figure 9:8 Percentage of other schools' competition posters per topic (Recommended implementation): Cycle 2
When message adoption is rejected, or slow, more creative presentation of the lessons and repeated exposure may improve results. This will be an issue of interest in forthcoming cycles. Learners from School D also neglected the topic of cyber citizenship; this was to be expected, however, as limited coverage of this topic occurred in the educational resources.

**9.5.2.2.2 Teacher-oriented implementation**

Both School AA and School BB were exposed to the educational resources and non-standard lessons conducted by their teacher’s. Students at School AA had been exposed to four lessons, while School BB had been exposed to two. The percentage of each school’s competition posters depicting content from each topic is provided in figure 9.9. The topics which learners preferred to depict were quite different in the two schools.

School AA’s learners produced posters depicting messages from most of the topics, while learners from School CC used mainly messages relating to the cyberbullying topic (64%, 66 of 103). These learners had been exposed to the same resources therefore the differences in measurements may have been attributable to the topics teachers focused on or the topics which learners found most relevant. School CC’s teacher had placed emphasis on cyberbullying as a topic in lessons, and the results showed that the majority of learners taught by the teacher had selected this topic for their posters. This topic was also particularly relevant to these learners as incidents of cyberbullying had occurred amongst their peers.

Similarities in the analysis of posters found that neither school had submitted posters containing messages on the topics of piracy or hardware security. Both these topics were focused on in depth in the expert presentations included in the recommended campaign solution but only briefly mentioned in the printed educational resources. This since neither school had an expert presentation this lack of coverage was understandable.

The lack of coverage of piracy and hardware security was also a trend in data from School AA. The drop in hardware security coverage reflects limited coverage of the topic. This was the school’s second year of exposure to the campaign, although the first time these particular learners had participated. The percentage of posters per topic in School AA’s entries differed considerably in Cycle 1 and Cycle 2 in all other respects.
Figure 9:9 Percentage of other schools’ competition posters per topic (teacher-oriented implementation): Cycle 1 – Cycle 2
In Cycle 1, the commonest topic in School AA’s posters was cyberbullying (48%, 58 of 122), followed by moderate coverage of cybercrime (22%, 27 of 122) and information and password security (24%, 29 of 122). By comparison, in Cycle 2, the commonest topic was information and password security (28%, 25 of 90), as in Cycle 1. The percentage of posters addressing cyberbullying (16%, 14 of 90) dropped significantly but there was moderate coverage of all topics, excluding piracy and hardware security.

The fact that coverage of campaign topics in School AA’s submissions was more widely distributed may be attributed to the extra printed materials that were provided in Cycle 2. More content was devoted to the various topics, and as a result, learners may have found topics more relevant. The of emphasis the teacher placed on topics may also have differed between cycles.

9.5.2.2.3 Limited implementation

School C participants engaged in self-study using the printed SACSAA educational materials that had been posted the school noticeboards. Both posters displayed a single topic; one depicted an anti-cyberbullying message and image, and the other illustrated and warned against the dangers of online activities. Both topics were featured in the materials. These topics may have been selected because they are commonly significant for children. In addition, both messages were included and covered by several campaign resources. No further analysis could be conducted.

9.5.2.3 Internalisation of Cybersecurity and Cybersafety Message(s)

The customisation and contextualisation of the campaign materials was effected to improve or increase the degree to which learners would internalise the campaign's cybersecurity or cybersafety messages. This was particularly apparent in the expert presentation. The increase in the number of resources which addressed the campaign topics and the increased involvement of teachers (educational experts) in the cybersecurity education process was also aimed to contribute to improved internalisation. This section discusses the outcomes of learners' internalisation of topics in Cycle2’s implementation.

9.5.2.3.1 Recommended implementation

The majority of School B (83%, 85 of 102) and School D’s (84%, 59 of 70) submissions suggested that campaign messages had been internalised to some degree. In addition, the majority of each school’s internalised posters included content that was depicted in a way that suggested full
internalisation (Figure 9.10). Only a few learners from both schools did not internalise the messages. In the case of School B, the majority of uninternalised posters were submitted by younger learners (ages 6–7). In School D, most uninternalised posters could not be interpreted because of poor artistic skills.

Figure 9:10 How well other schools’ learners internalised the cybersecurity or cybersafety messages (recommended implementation): Cycle 2

As this was the first year of participation for both schools, results could not be compared to Cycle 1’s results. However, based on the analysis, Cycle 2’s recommended campaign implementation appeared very effective at encouraging learners to internalise their selected campaign messages to some degree. Overall, there was trend indicating that most learners had internalised the messages and had begun to or had fully contextualised and internalised the campaigns messages.

A point of interest was that as in School A’s results, most of posters which indicated that learners had fully internalised the campaign’s messages used topics that had been emphasised in the expert presentation. This may indicate that the highly contextualised expert presentation affected how well learners internalises the campaign’s messages.
9.5.2.3.2 Teacher-oriented implementation

On the whole, results indicated that most learners at both high schools had internalised the campaign’s messages to some degree. Very few learner posters reflected a lack of internalisation of the depicted messages.

The submissions from both schools were difficult to analyse in terms of internalisation. Both had submitted digital posters, many of which comprised “copy and paste” images. The posters also tended to be very simplistic as if the learners had not had a lot of time to create them or had simply not been interested enough to make more of an effort. There was a definite lack of creative design and as a result posters were generic or very similar. The measurements reflected in Figure 9.11 are based on the researcher’s interpretation of each poster combined use of the images and included text. However, based on feedback from involved teachers, the researcher believes that the majority of learners had fully internalised the campaign messages; this internalisation was simply not reflected in the posters, however.

![Figure 9.11 How well the other schools’ learners internalised the cybersecurity or cybersafety messages (teacher-oriented implementation): Cycle 1 - Cycle 2](image)

Figure 9.11 reflects how well messages depicted on School AA’s and School BB’s posters were internalised. Overall, these results indicate that most learners at both high schools had internalised the campaign’s messages to some degree. Very few learners’ posters indicated a lack of internalisation of the depicted messages.
Feedback from the teachers at both schools indicated that the learners had not found the material challenging. The learners had gone through the motions of participating, but had not been truly engaged or had their interest captured. This may have led to a disinterest in contributing to the campaign by creating expressive or detailed content for their posters. This result contrasts starkly with Cycle 1’s results. In Cycle 1 learners from School AA had been engaged and had actively taken part in the campaign. As a result, their poster entries suggested that most of the campaign messages had been fully internalised by learners. The campaign may have affected the audiences differently for many reasons examples, including:

- The campaign and its content may have been more novel to Cycle 1’s learners.
- Different learners may have completely different learning objectives and/or styles.
- The changes and additions to materials may have appealed more to primary school learners.
- The content may not have been challenging enough for learners to engage them.

Whatever the reason for this lack of engagement, the results showed that in contrast to Cycle 1, significantly fewer high school learners had fully internalised their depicted campaign messages. This may suggest that different educational resources or approaches and measurement tools are necessary when targeting older learners.

9.5.2.3.3 Minimal implementation

Both submissions from School C were fully internalised. This indicated that the educational materials to which learners had been exposed on the notice boards were effective at communicating their content. No additional analysis could be conducted.

9.5.2.4 Presence of Brand Symbols

This measurement examines the presence of brand symbols in submitted posters. In Cycle 2’s campaign implementation most of the educational resources, particularly the expert presentation, included the SACSAA logo as the brand symbol of choice. Learners were encouraged to notice it and make use of this logo in their posters.
9.5.2.4.1 Recommended implementation

None of the posters from School B and School D contained any brand symbols. Based on their absence, the expert’s observations during the presentations and the teacher’s feedback, it would appear that learners at these primary schools did not relate to the logo. Cyber Sid, the mascot, was present in some of the printed materials was not highlighted or discussed. Neither school had been previously exposed to Cycle 1’s introduction. This confirms that a passive presence of a mascot does not appear to have an immediate impact on learners. The results also suggest that if learners do not relate to a brand symbol, even if it is discussed, it will not be adopted. Aaker and Joachimsthaler (2000) confirm this by showing that if consumers have strong feelings then they will create favourable perception of the brand and are more likely to adopt the branding symbols. The expert presentation included a discussion of the logo, its meaning and relevance; nonetheless, the symbol was not featured on any of the posters.

Most posters from School B were hand-drawn so they could easily have included drawings of the brand symbol. In the case of the remaining, digital entries from School B and all School D’s posters even though brand symbols were made available to learners, none of them opted to include these images.

9.5.2.4.2 Teacher-oriented implementation

None of the entries from either school included the campaign’s brand symbols. School AA’s learners had not included brand symbols in Cycle 2 either. A possible reason for this absence in that Cycle 2 was the lack of easy access to the symbols. Digital copies of the images were made available for download from the SACSAA website, and had been provided to teachers. Thus, although the learners had access to the images, none of them included them.

Feedback from teachers indicated that the brand symbols had not been highlighted; however, they had provided their learners with access to the images. This result indicates that the passive presence of the branding (SACSAA logo) did not attract learners’ attention, interest, or consideration.

9.5.2.4.3 Minimal implementation

School C was the final primary school. Neither of its poster entries featured brand symbols, although they were included on the displayed educational resources. This may indicate that the
presence of the symbols alone may not be enough to encourage learners to associate them with cybersecurity. It may also indicate that these brand symbols simply did not appeal to learners or register as being important or relevant. No additional analysis could be conducted.

9.5.2.5 Additional evaluations of pedagogically sound cybersecurity education game (Cycle 2)

This measurement was taken to validate the findings of the Cycle 1 study of the “Snakes and Ladders” games at School A. The study was implemented at two additional schools, School B, and School D. If playing the game had a positive effect on learners’ knowledge, then the game could be confirmed as an effective education tool that could be used as part of the SACSAA campaign’s educational resources.

This section presents the results of the evaluation of the game, based on the procedure described in section 9.4.2.1.1 and Appendix E. These results were published in Reid & Van Niekerk (2014b).

The results show the percentage of learners from each school who answered the assessment questions correctly in the pre-play, post-play, and follow-up assessments. Appendix E provides the wording of the questions in each assessment.

In order chronological order, each assessment’s questions dealt with the following cybersecurity password management messages:

1. Never write your password down.
2. Trust your parent or guardian with your password.
3. Use special characters and numbers to make your password secure.

This section will discuss the results from each school, and an overall finding based on the results of Cycle 1 and Cycle 2’s evaluations of School B and School D.

9.5.2.5.1 School B

Figure 9.12 shows the percentage of learners from School B who answered the assessment questions correctly at each assessment stage.

Initially, the results of pre-play assessment showed that most learners knew that they should never write their password down (67%, 6 of 9) and to make use of alphanumeric characters and symbols to create a strong password (56%, 5 of 9). However, very few learners knew that they
should only trust their parents or guardian with their password (22%, 2 of 9). Many learners indicated that they would share their passwords with anyone who shared their own with them.

Figure 9:12 Percentage of School B’s learners who answered each assessment’s questions correctly

The post-play assessment results revealed that playing the game had an immediate (confirmed short-term) impact on learners’ knowledge about the password security lessons. All the learners were aware that they should not write down their passwords (100%, 9 of 9), and that they should create strong passwords using alphanumeric characters and symbols (100%, 9 of 9). Most of the learners were also now aware that they should only share their password with their parents or guardian (89%, 8 of 9). Overall, the post-assessment findings were consistent with what had been observed in the evaluation of School A’s learners (section 8.5.1.6).

The follow-up assessment showed that there had even been a further improvement in learners’ knowledge of the selected password security lessons. Learners answered all questions correctly. These learners had not been exposed to additional cybersecurity education between the post-play and follow-up assessments. The improvement in their results may be attributable to further contemplation of the lesson and/or discussions amongst themselves in the time between assessments. Overall, the follow-up-assessment findings were also consistent with what had been observed in School A’s evaluation (section 8.5.1.6).
9.5.2.5.2 School D

Figure 9.13 shows the percentage of School D learners who answered the assessment questions correctly at each assessment stage. Overall, the results were similar to those of School B.

![Graph showing percentage of learners who answered questions correctly](image)

**Figure 9.13 Percentage of School D’s learners who answered each assessment’s questions correctly**

In the pre-play assessment, most of the students answered Question 1 (53%, 8 of 15) and Question 3 correctly (67%, 10 of 15), while a minority (27%, 4 of 15) answered Question 2 correctly. In the post-play assessment, the majority (93%, 14 of 15) answered Question 1 and Question 3 correctly. There was a considerable increase on the number of students who answered Question 2 correctly (73%, of 15). In the follow-up assessments, the percentage of learners who answered Question 1 and Question 3 correctly remained consistent. There was a further increase in the percentage of the learners who answered Question 2 correctly (87%, 11 of 15). These findings were consistent with the findings of the other evaluations at School A and School B.

9.5.2.5.3 School A, School B, and School D

Overall, the results for all three evaluations of the “Snakes and Ladders” game showed that playing the game had a positive effect on learners’ knowledge. The initial finding from School A (section 8.5.1.6) was confirmed by the results of School B and School D. The consolidated results
of each assessment for all schools that had participated in the various campaign cycles are shown in Appendix D Table 1.

Overall, these results allowed the researcher to conclude that the game was an effective education tool which could be used as part of the SACSAA campaign’s educational resources.

The first set of results of the game evaluation conducted as a case study at School A was presented at the Kaspersky “Cybersecurity for the Next Generation” Student Conference: Asia-Pacific & MEA in Singapore. Those results and the results of the additional evaluations were included in a conference paper presented at the 8th IFIP WG 11.8 World Conference on Information Security Education and in a journal article published in *Information Management & Computer Security* (Reid & Van Niekerk, 2013a, 2014b).

Section 9.5.2 discussed the results from Cycle 2 of the action research process for all schools (except School A) that took part in the 2013 SACSAA education campaign and poster competition. The next section will present the general results of this research cycle’s campaign.

### 9.5.3 General Results

The schools that participated in Cycle 2’s campaign and competition discussed above were School A, School B, School C, School D, School AA and School CC. This section discusses the general results of the game, examining all the data gathered collectively. The general trends in participation numbers, the number of posters depicting each topic, the degree of internalisation of campaign messages and the presence of brand symbols in the posters are discussed.

#### 9.5.3.1 Learner participation

Cycle 2 showed a large increase in the number of participants in comparison to Cycle 1. In Cycle 2, a total of 424 learners from various schools participated. Six schools took part. Four were primary schools, with a total of 231 participants. The remaining two schools were high schools and had a total of 193 participants. The distribution of the learners among the schools is as follows:

- School A – 57
- School B – 102
- School C – 2
- School D – 70
School A (primary school) and School AA (high school) were the only schools participating for a second time and learner participation decreased in both. This was attributed to outside factors which were beyond the campaign’s control, as discussed on 9.4.

School and learner numbers were the highest thus far in the campaign. This year schools all received personalised invitation packs. Most schools that participated had also been visited by a campaign representative for an introductory and explanatory meeting. This meeting took place with the representative, the principal, and/or the teacher(s) involved in implementing the campaign at the school. Feedback from teachers indicated that these visits and the invitation were significant contributors to the school’s decision to participate in the campaign.

An issue of interest for Cycle 2 was whether the value of the prizes had an influence on participation. Feedback from teachers indicated that their learners had considered the prizes as motivation to participate; however, this was not the primary motivator. All teachers said that their learners had indicated that the teacher and peer encouragement had primarily encouraged them to participate in the competition component of the campaign. At schools that were exposed to expert presentations, this, and the possibility of having their work included in calendars and materials was also credited with attracting learners’ interest in participating.

### 9.5.3.2 Posters per topic

The measurement aimed to determine which topics learners related to and adopted, based upon the depictions of messages on their posters. On an individual school basis, this measurement was used to determine whether the emphasis placed on topics by material and activities was reflected in the learners’ posters (section 9.5.1.2 and section 9.5.2.2). This section focuses on whether there were any trends regarding topics featured on posters in Cycle 2, and how this compared to Cycle 1 (figure 9.14). It also examines whether there was difference in topic focus between primary schools and high schools (figure 9.15).

Overall, four trends were evident in the results. Of the 424 submitted posters, 80% (339 of 424) depicted a single topic, with the remaining 20% (85 of 424) using multiple topics. The first trend was thus that there was a slight general increase from Cycle 1 to Cycle 2 in the percentage of posters depicting a single topic rather than several topics. Previously, 76% (165 of 217) of Cycle 1’s posters had reflected messages from a single topic. In Cycle 2, most of the posters that
depicted a single topic used anti-cyberbullying messages. This trend linked to an overall increase in the percentage of the posters featuring cyberbullying messages in Cycle 2.

The analysis of Cycle 2’s data showed that, when comparing data from the two cycles, there was no major shift in the percentage of posters that had used each topic. This was the second topic-related trend. In both cycles, the most frequent topics were:

- cyberbullying – 38% (Cycle 1), 43% (Cycle 2)
- information and password security – 35% (Cycle 1), 28% (Cycle 2)
- stranger danger – 23% (Cycle 1), 17% (Cycle 2)
- social networking – 16% (Cycle 1), 10% (Cycle 2)

The topics used least (in ascending order) remained constant:

- piracy – 0% (Cycle 1), 0.24% (Cycle 2)
- hardware security – 2% (Cycle 1), 1% (Cycle 2)
- browsing and downloading – 2% (Cycle 1), 2% (Cycle 2)

This trend supports the assumption and the brain-compatible principle that learners will focus on topics that are most contextually and personally relevant. The most depicted topics were those one would expect learners to be familiar with and to relate to. Similarly, the relative neglect of piracy and dangers of browsing and downloading messages was also anticipated, given that these relate to obtaining games, films, and series free of charge.

The third noticeable trend in the general results was the difference between Cycle 1 and Cycle 2 percentage of topic depiction barely changed. This trend was pronounced even though the general order of most and least depicted topics did not change. There were noticeable increases and decreases in the exact percentage of posters that covered each topic. The percentage of posters that included the topics of cyberbullying, dangers of online activity and piracy increased to various degrees. In the case of the remaining topics, the number of posters decreased.

The topic of cyberbullying had the most noticeable increase in the percentage of posters depicting its messages. Many of these posters contained a single topic, focusing solely on anti-cyberbullying messages. The increase in anti-cyberbullying messages may relate to the increased focus on this topic in the materials and expert presentations. Similarly, the slight increase in the use of anti-piracy messages may also be linked to the message in the materials being accepted by part of the target audience. This constitutes an improvement on Cycle 1’s results.
Figure 9:14 Percentage of all schools’ competition posters per topic: Cycle 1 – Cycle 2
Figure 9:15 Percentage of all schools’ competition posters per topic (Primary Schools vs High Schools)
Overall, the results indicate that if the campaign places emphasis on specific content in materials that is relevant to and aligned with learners' views or beliefs, such learners will accept the campaign’s messages. This acceptance is then visible in the measurement of topic coverage, e.g. cyberbullying. However, the results also indicate that even if there is significant coverage of a topic, but it is contrary to learners' beliefs or preferences, the message may be rejected. This rejection is measurable in its absence of depiction or in the use of contrasting messages such as piracy. Therefore, simply increasing a topic’s coverage does not guarantee acceptance off the message; nonetheless, continued coverage of the content over time may result in the its gradual acceptance, as in the case of piracy over the two cycles.

The fourth trend was that certain topics were more relevant and more often used by particular age groups (primary school learners as opposed to high school learners, for instance). There were considerable differences in the percentage of primary school and high school posters illustrating messages on the following topics:

- Stranger Danger – 24% (primary school posters), 9% (high school posters)
- Dangers of Online Activities – 13% (primary school posters), 5% (high school posters)
- Information and Password Security – 36% (primary school posters), 17% (high school posters)

A higher percentage of primary learners used these topics. As previously discussed, learners tend to illustrate messages that are most familiar or relevant to them. Based on their typical online activities, high school learners would be likely to have a broader range of knowledge and to be more familiar with these of the topics than primary school leaners. Thus, their messages would illustrate any or many of the topics. On the other hand, primary learners would be familiar with and able to relate to a more limited number of the topics. This might align with Cycle 2’s finding that a higher percentage of primary school learners chose these particular topics.

### 9.5.3.3 Internalisation of Cybersecurity or Cybersafety Message

The measurement determined the degree to which the learners had internalised the cybersecurity or cybersafety messages which they depicted in their posters. Differences between Cycle 1 and Cycle 2’s measurements were expected to show whether the customised and contextualised materials and activities had affected the degree to which the learners had internalised this content. This customisation and contextualisation was provided to different degrees by the expert presenters and/or teachers at each school. The degree to which the materials were customised
and contextualised was dependent on the campaign’s implementation format and the individual decisions made by experts and teachers.

Schools that followed the recommended implementation were exposed to relatively similar degrees of customisation and contextualisation of materials and activities. This was because the researcher primarily conducted the presentations. The researcher sought to provide equal learning opportunities to all target audiences, while at the same time meeting each audience’s special needs. By comparison, at the schools where the campaign was teacher-oriented, the degree and types of customisation and/or contextualisation varied as the teachers were not provided with specific guidelines on how to implement the modifications. This measurement is therefore difficult to make definitively when discussed from a general perspective.

The measurement was thus analysed from two viewpoints. The first analysis examined the differences between internalisation of the material’s content based on the analysis of the all participating learners’ posters from Cycle1 and Cycle 2 (figure 9.16). The second analysis involved a comparison of the degrees of internalisation among primary school learners and high school learners (figure 9.16). This measured general trends regardless of sub-characteristics of the target audience. This analysis provided an opportunity to compare the results for the different age-groups.

Figure 9.16 How well all the schools’ learners internalised the cybersecurity or cybersafety messages: Cycle 1 – Cycle 2
The first analysis to be discussed is the comparison of Cycle 1 and Cycle 2's results. Figure 9.16 shows that in Cycle 1, a high percentage of 97% (210 of 217) of the learners internalised the campaign messages, while in Cycle 2 87% (367 of 424) of the learners had internalised the campaign message. Cycle 1 and Cycle 2’s data showed that the overall percentage of students who had internalised the campaign’s messages to some degree decreased (figure 9.16). However, numerically there was an increase. The number of learners participating each cycle varied, thus a numerical comparison was difficult to analyse and compare.

Cycle 1 involved two campaign implementation formats and three schools, two of which were high schools, and a small target audience of 217 learners. Cycle 2 had three general implementation formats, a larger target audience (424 learners, five schools), mostly young primary school learners. The scope of the campaign and the level of education the learners had received was more varied in Cycle 2. However, the interventions of customising and contextualising the material when possible influenced a larger number of the learners to internalise the material to some degree. Therefore, despite the overall drop in the percentage of learners who internalised the campaign messages, this campaign cycle is considered very successful.

The percentage of learners who demonstrated each level of internalisation was more widely distributed in Cycle 2 than in Cycle1. In Cycle 1, the majority (75%, 164 of 217) of learners had fully internalised the messages. The remainder were distributed over the other internalisation levels. In Cycle 2, a smaller majority (46%, 196 of 424) had fully internalised their depicted messages and the remaining students were similarly distributed over the other internalisation levels. Of the remaining Cycle 2 learners who had internalised their depicted messages, 18% (78 of 424) could rephrase their messages and 22% (93 of 424) depicted the messages as they were provided in the materials. Cycle 2’s more widely distributed internalisation levels were attributable to the varied implementation formats and the larger target audience.

From a general perspective, Cycle 2 was more representative than Cycle 1 of how a national campaign could realistically be implemented. The materials were a constant but access to them, customisation and contextualisation and details of the implementation were content, context and implementation specific. Uniformity in the campaign’s implementation and complete success are unlikely in first campaign cycles, although they can be targeted objectives.

---

3 Reflecting upon the whole campaign history (2011-2015) the 100% internalization rate of high school learners in Cycle 1 was an anomaly.
A similar trend emerged from Cycle 2’s results. The wider distribution over levels of internalisation in Cycle 2’s measurement may have been the result of a larger audience being exposed to a more realistic implementation of the campaign. Cycle 2 was more reliant on the materials, resources, and different implementations of the campaign. Future campaigns will be more likely to show similar implementation processes to Cycle 1 than Cycle 2. Thus, effects of future improvements are anticipated to be more perceptible and more comparable in future campaign cycles’ results.

This concludes the discussion of the results of the first analysis. The second analysis to be discussed is the comparison of the measurement of primary school learners and high school learners’ internalisation in the Cycle 2 campaign (figure 9.17). These results are presented alongside the aggregated levels of internalisation for all learners from Cycle 2.

![Figure 9:17 How well primary school and high school learners internalised the cybersecurity or cybersafety messages: Cycle 1 – Cycle 2](image)

Of the 231 primary school learners participating in Cycle 2, 84% (193) internalised the messages depicted on their posters. By comparison, of the 193 high school learners from Cycle 2, 90% (83) internalised the messages depicted on their posters. This result shows that a greater number of older students internalised the materials in both cycles. Based on feedback provided by teachers from the various schools, it appears that younger learners were positively challenged by the material, but older learners found the material easier and were less engaged because of the lack of challenge it presented.
Overall, in Cycle 2 as in Cycle 1 a higher percentage (90%) of high school learners internalised materials than primary school learners (84%). The positive trend in students’ internalisation of the material was continued from Cycle 1. However, unlike Cycle 1, in Cycle 2 more primary school children (49%) had fully internalised their depicted messages than high school learners (43%).

In Cycle 2, both school levels showed a decrease in the percentage of learners who fully internalised the materials, while the percentage of learners who had not internalised the material increased. Numerically most of measurements showed greater numbers students than Cycle 1. In Cycle 2, 49% (113 of 231) of primary school learners had fully internalised their depicted messages; this is comparable to Cycle 1’s result of 52%(49 of 94) of the primary school learners. Similarly, in Cycle 2, 53% (83 of 193) of high school learners had fully internalised their depicted messages, comparable to Cycle 1’s result of 94%(115 of 123). The differences in percentage can be attributed to the larger size of the overall target audience and campaign implementation formats.

The increased percentage of posters that reflected “un-internalised” messages was related to the increase in digitally created posters. In primary school entries, there was an increase in digitally created posters (e.g. using Paint and PowerPoint applications). The majority of the un-internalised posters were digital posters and were categorised as being either indecipherable or designed in a that they could not be interpreted taking a stance regarding their message(s). In the primary schools, the un-internalised posters increased from 7% (7 of 94) to 13% (38 of 231). These included digital posters and posters submitted by extremely young participants (aged 5–7). Amongst the high school learners, the un-internalised posters increased from 0% to 10% (19 of 193). These posters were all lacking a stance or definite interpretation of meaning. The posters consisted mainly of downloaded and pasted images.

At both school levels, the percentage of posters which depicted the messages also increased in comparison to Cycle 1. The percentage of primary school learners increased only slightly from Cycle1’s 14% (13 of 94) to Cycle 2’s 15% (24 of 231). This indicates that learners in this age range were engaging with the material and internalising it at a higher level than basic acceptance of the messages. This material was therefore suitable for them.

On the other hand, the percentage of high school learners who accepted the message as given instead of further internalising it increased dramatically. The measurement increased from Cycle 1’s 3% (4 of 123) to Cycle 1’s 31%(59 of 193). Similarly, the measurement of high school learners who merely rephrased the campaign messages increased from 3% (4 of 123) to 17% (32 of 193).
The high school teachers had indicated that learners were not engaged or challenged by the material. A corresponding lack of effort was demonstrated in their posters. This resulted in only basic interpretations or repetition of the campaign’s messages as provided in the materials. This result suggests that more challenging material is required for older learners.

Factors that contributed to the considerable differences between the two cycles’ results in this regard were, firstly, that the number of high school learners participating in Cycle 2 (193) was greater than in Cycle 1 (123). Therefore, there was a larger, more varied audience at which to pitch the campaign messages. The implementation of the campaign may not have been ideal for all learners. Secondly, the audiences consisted of students with different pre-existing knowledge in each cycle. Thus, the degree to which learners could relate to the concepts differed. Thirdly, in both cycles, high school learners were exposed to teacher-implemented campaign formats and were not to expert presentations. The fourth and final factor builds upon the third: the main alteration to Cycle 2’s campaign implementation was the additional course materials and the customisation and contextualisation of the material. In the teacher-oriented and limited campaign implementations, teachers were responsible for this customisation and contextualisation. The degree to which teachers implemented and reported customisation and contextualisation was not regulated or directly monitored by the researcher. Future campaigns should provide guidelines for this contextualisation and customisation.

9.5.3.4 Brand Identity

This measurement’s main aim was to determine whether the impact of the brand symbols used in the campaign materials would be such that learners would:

- Be conscious of the branding
- Include the branding in their own posters
- Associate the branding with the campaign’s messages.

Figure 9.18 shows the results of the analysis of Cycle 1 posters versus Cycle 2 posters for this measurement. Cycle 2 used the SACSAA logo as the primary brand symbol. The Cyber Sid mascot appeared only on the Cybersecurity Pledge form (figure 8.4, section 8.3.2.1.3). School A was the only school previously exposed to the Cyber Sid Mascot.

Overall, the percentage of learners who identified with the brand symbols decreased in Cycle 2. The percentage of posters that did not include any form of branding increased from Cycle 1’s 86%
(65 of 94) to 96% (408 of 424) in Cycle 2. In addition, the percentage of posters including either the mascot or the SACSAA log or both also decreased. An interesting trend which emerged was that despite the SACSAA logo being the primary logo and most emphasised symbol in the campaign, the Cyber Sid mascot was the most depicted brand symbol in Cycle 2. This could only be attributable to past exposure to the mascot or learners noticing the mascot on the pledge flyer. Based on these results, the use of the SACSAA logo as the brand symbol was not particularly successful in attracting and engaging the learners.

![Figure 9.18 Percentage of all schools' posters depicting brand symbols: Cycle 1 – Cycle 2](image)

Another further of this measurement was to determine whether different branding appealed to particular audiences or subgroups within the target audience. Figure 9.19 provides a comparison of the results of this measurement for posters submitted by primary school learners versus high school learners.

The brand symbols were not adopted (depicted in the posters) at all by high school learners. All their entries were digitally created. Despite the researcher providing increased access to the brand symbols via the Cyberaware website, the learners did not include them in their posters. This result suggests that the branding did not appeal to older learners.

In the primary school category, the only school to adopt the group was School A. These results are discussed in section 9.5.1.4.
Overall, the general findings for this measurement were that there was very low brand awareness, currently localised to a single audience. The Cyber Sid mascot was considered more relevant to the audience that had been exposed to both brand symbols in a similar manner (in the recommended implementation) over two years.

Section 9.5.3 presented the general results from of the action research process Cycle 2 for all schools participating in the 2013 SACSAA education campaign and poster competition. This concludes the results section for Cycle 2. The next section presents the researcher’s reflections on the lessons learnt from this cycle of the campaign.

### 9.6 Reflections

This section discusses Cycle 2’s reflections and lessons learned from the implementation of the SACSAA campaign in 2013. It first reports the reflective thoughts and lessons learned because of actions taken to meet the Cycle 2’s issues of interest and their related objectives. These reports are presented in the order in which the objectives were introduced in section 9.2. Additional lessons learned in the implementation of the campaign but not specifically related to objectives are presented afterwards.
9.6.1 Establish a more formalised education approach with supporting materials

The first issue of interest was the need for a formal, pedagogically sound education effort to raise awareness and educate learners about cybersecurity and cybersafety. This is an issue of interest that has been explored since Cycle 1 (C1O1). The actions implemented for C1O1 continued in Cycle 2 but were enhanced by C2O1 and C2O2. The actions and reflections relating to these Cycle 2 two objectives are discussed below.

C2O1 was to:

“Provide further formalised, pedagogically sound educational resources.”

The first action taken to meet C2O1 was the inclusion of the additional 101 flyers with separate 101 topics (Figure 9.2) and the NMMU SACSAA calendar (Figure 9.3). These resources were included as they were in keeping with some BCE education principles and they provided additional content that was more topic specific. The purpose of the material was to provide the learners with more content and more learning opportunities. Based on BCE 1, providing more learning opportunities was expected to assist learners to experience and internalise the campaign content’s messages. This would make the campaign more effective.

Based on feedback received from teachers learners did make use of the multiple resources. The results show that the majority had to some degree internalised the material’s messages depicted in their posters. In addition, the majority of these learners had fully internalised the messages. The additional pedagogically sound resources contributed to these results.

The second action taken to meet this objective was the modification of the expert presentations that were implemented at School A and other schools which followed the recommended campaign implementation. Various elements of the expert presentation were modified to comply with a few Cycle objectives. Modifications which are relevant to C2O1 were the presentation and delivery changes aimed to make the presentation comply with the recommendations of BCE principles. Modifications included increased interactive discussion and activities; the contextualisation of the content and the inclusion of some media.

Both actions taken to meet C2O1 and the consequent results of the campaign contributed to reinforcing Lesson 7.
C2O2 was to:

“Enable a further formalised education process by increasing the role of the expert educators (the teachers) in the educational component of the SACSAA campaign.”

Cycle 1’s results showed that schools where teachers were involved in promoting the campaign had a higher number of participants than schools without teacher involvement. C2O2 aimed to take advantage of this finding.

The first action taken to increase the role of the educator was to ask teachers to specify which cybersecurity and safety topics they believed were most relevant to their students. This enabled the teacher and expert to collaborate in contextualising the expert’s presentation to make it as relevant to their learners as possible. This action is discussed further in relation to C2O6.

The second action taken to meet C2O2 was a request made in the invitation to participate in the campaign. Two requests were made of the teachers to:

1. incorporate the resources into at least one of their own lessons
   This request was made for several reasons. Firstly, if complied with it would result in the material being covered by an educational expert. This would thus make use of an existing educational resource to achieve the campaign’s educational goal. Secondly, in the case of recommended campaign implementation, this would provide repetition and reinforcement of the expert lectures. Thirdly, this would provide teachers and learners with the opportunity to contextualise the content in relation to their lesson and own contexts. These actions would encourage the learners to internalise the content’s messages.

2. encourage their students to participate in the campaign
   This request was made to make use of Lesson 9. Having the teacher show support of the campaign firstly shows the learners that it is an officially accepted campaign and topic. Secondly, it provides a “trusted” individual with an opportunity to encourage the learner to take part. Learners would typically be expected to comply with a request from someone they know and (or) trust rather than a single, simple competition advertisement.

Schools that followed the recommended or teacher-oriented campaign implementations complied with these requests. Feedback indicated that frequently teachers included the materials in several lessons, and some even customised the examples so that they would be more relevant to their learners. These schools had much higher numbers of participants than schools where teachers
or experts were not involved. In addition, the percentage of all learners who internalised the message was high.

These results indicate that increased teacher involvement had an impact on participation rates in the competition. The more “formalised” classes in which the resources were used proved more effective at educating learners than simply providing access to the materials. The content often appeared in the posters as it was focussed on in the materials (discussion continues in relation to C2O7).

These findings thus validated Lesson 9 and Lesson 11. Teachers are the campaign’s allies and a resource waiting to be used. They can represent the campaign and its messages to a greater degree than the campaign experts would ever be able to achieve. They can present material in the school, and potentially contextualise their teaching of these materials if they are provided with sufficient educational resources. They can “champion” the campaign at their schools, or nurture learner champions (Atkinson et al., 2009). This, in turn, can provide an opportunity to increase the percentage of learners who internalise the campaign’s message.

Future iterations of the campaign should aim to involve teachers even further in the campaign. Many of the teachers indicated in their feedback that they were would be willing to become more involved in implementing the campaign in their classes or at their schools. However, some feedback indicated that developing lesson plans on campaign topics and so on was limiting their activities in their subject area.

Making use of existing resources and experts (Lesson 12) was strongly supported by the results of actions taken to meet C2O2. However, if the campaign does not sufficiently support the experts they cannot provide optimal assistance. This finding has resulted in the initial formation of another lesson. Lesson 14 is that:

\[
\text{Lesson 14} \\
\text{Campaign role-players must be provided with appropriate and sufficient resources to fulfil their role effectively.}
\]

Providing the teacher with more formalised tools for classwork, for instance a curriculum, could increase the number of teachers who would use the material in their own lessons. It might also enable teachers to have a more consistent or improved impact on learners’ knowledge. The effect of providing a formal curriculum will be an issue of interest for the next campaign cycle.
9.6.2 Examine the effect of method(s) used to achieve school participation and gain learners’ attention

The second issue of interest was the methods used to gain learners’ attention in and participation in the cybersecurity education campaign and poster competition. Cycle 2 continued to implement the marketing and branding practices of previous iterations. Practices recommended by Lesson 2, 8, 9 and 10 were all implemented. This resulted in increased participation and reconfirmed the lessons’ validity. In Cycle 2, two issues of interest were the role of brand symbols (C2O3-C2O3A4) and the value of prizes (C2O4).

In Cycle 1, Lesson 10 was learnt initially. The focus on branding in Cycle 1 was to compare the passive versus active introduction and inclusion of the brand in the campaign material and activities. The active inclusion of the brand was found to be more effective; Cyber Sid was more frequently featured in competition posters where learners had been introduced to the mascot. On the issue of attracting learners’ attention, the first issue of particular interest in Cycle 2 was to test further the validity of Lesson 10’s stipulations that design of a mascot matters and that mascots should be actively incorporated into campaign materials and activities. This led to C2O3 and C2O3A.

C2O3 was to:

“examine whether the choice of brand symbol included in the educational campaign affects the adoption of brand symbols.”

As explained in the branding description in section 9.3.2.3, this objective was met in stages. Stage 1 was Cycle 1’s finding that Cyber Sid, which had been more thoroughly introduced and actively included in campaign material and activities, had a higher adoption rate than the SACSAA logo. The action taken in Cycle 2 was to determine whether the actions conducted with Cyber Sid would work for the SACSAA logo. Therefore, Cycle 2’s campaign implemented the active introduction and primary use of the SACSAA logo in all campaign materials and activities.

Unfortunately, the percentage of learners who identified with the brand symbols decreased. The campaign results showed that most learners did not include brand symbols on their posters. In fact, only some primary school learners included them. This indicates that particular subgroups within the overall target audiences may be more open to accepting or more able to relate to branding or particular brand symbols than other groups.
Among those posters that included brand symbol(s), more included the Cyber Sid mascot than the SACSAA logo. This finding indicates that if even if the same introductory and usage procedures are followed, when a brand symbol is not relevant to an audience it will not be accepted. Alternatively, it may take them longer to accept the branding than a more relevant symbol. This finding indicates that the choice of brand symbol design is important, supporting Lesson 10. A sub-lesson to Lesson 10 is, therefore, that:

Sub-lesson 10a

Branding design for cybersecurity campaigns should take into consideration the relevance of the design to the target audience

This sub-lesson will be explored further in Cycle 3.

The above results and findings will now be discussed in relation to C2O3A which was to:

“consider the impact of the selected brand symbol on the formation of a SACSAA campaign brand identity and recognition.”

The findings of Cycle 2 indicate that the character brand symbols were more relevant to primary school learners than high school learners. But this relation is currently low. Therefore, the choice of brand symbol and brand identity may take a longer period to become recognised and acknowledged.

The finding that the Cyber Sid mascot had a higher adoption rate than the SACSAA logo confirms that recognition of a brand symbol is linked to its relevance to the learner. This supports Lesson 10 and sub-lesson 10a.

This concludes the reflection upon the issues of interest relating to brand symbols. The reflection upon the other issue of interest regarding the value of prizes is discussed below.

C2O4 was to:

“investigate whether the value of prizes affects the level of learner participation in the competition.”

Previous campaign cycles found that prizes were regarded as a motivation for learners to participate in the poster competition. The issue of interest in Cycle 2 was whether the value (monetary) of prizes mattered to the participants. The action taken to meet this objective was to significantly reduce the value of the prizes in this cycle.
The level of participation was not lower than in previous cycles. Feedback from teachers indicated that prizes continued to motivate learners to participate. This finding has two possible reasons:

1. For learners, the value of the prize is less significant than winning; or
2. The value of cycle 2’s prizes was not low enough to deter participation.

The findings from the actions taken to meet C2O4 can be considered as supporting information for Lesson 12.

General findings from the Cycle 2 campaign relating to this issue of interest were the following:

- The increasingly active role of educators using campaign materials in class and encouraging participation attracted learner attention and gained their participation. This finding supports Lesson 3.
- Feedback from teachers at schools where the campaign was implemented was conducted according to the campaign recommendations, indicating that they considered the expert presentation effective in capturing ‘learners’ interest. This finding supports Lesson 3 and Lesson 8.

Overall, the analysis of the data found that although learner interest and participation in the campaign increased, this could not be attributed to the brand symbols included in the campaign.

**9.6.3 Re-evaluate the effectiveness of the cybersecurity education game**

The third issue of interest was the need to confirm or disprove the suitability and effectiveness of the pedagogically designed “Snakes and Ladders” cybersecurity game as an educational tool for a broadly defined audience.

C2O5 was to:

“re-evaluate the educational cybersecurity game to determine whether it is effective in educating learners from different target audiences and contexts”.

The action taken to meet C2O5 involved evaluating the game using the original evaluation procedure from Cycle 1 but with different target audiences. This evaluation was based on:

- the game’s impact on learner knowledge about password security management
- the teacher perceptions of the game’s effect on learner knowledge and behaviour.
Cycle 2’s evaluation of the game confirmed the findings from Cycle 1. The results for all three evaluations of the “Snakes and Ladders” game showed that playing the game had a positive effect on the knowledge of the learners concerned. This effect was measurable as short-term and long-term recall. Learners could consistently remember the password security lessons taught by the game. Feedback received from the teacher involved also indicated that learners had shown an increased level of awareness of the need for password management.

These results allowed the researcher to conclude that the game was an effective education tool for use as part of the SACSAA campaign’s educational resources. This conclusion supports Lesson 7.

### 9.6.4 Increase the relevance and relatability of the campaign and its content for the learners

Based on Cycle 1’s results, if learners were exposed to contextualised education material, then their own posters would reflect knowledge and understanding of the campaign’s information in a more contextualised format. The fourth issue of interest in Cycle 2 was determining whether providing highly contextualised and customised content would consistently result in learners developing and demonstrating a more personally contextualised understanding of the campaign messages.

*C2O6 was to*

> “design and implement the campaign and its content to be contextualised and customised to the target audience.”

The first action taken was the inclusion of relevant explanations and examples in the additional 101 flyers. These explanations were intended to help learners to contextualise the guidelines. The second action taken in meeting the objective was the inclusion in a calendar of the winning posters from Cycle 1. These posters were contextualised from the Cycle 1 participants’ point of view. Cycle 1 participants of similar age and similar cyber experience as the current target audience. As a result, their interpretations, and depictions of cybersecurity and cybersafety messages were similar. The third and largest action taken was the customisation of the expert presentation at each school that was following the recommended implementation. The expert customised the talk to address issues and examples that were familiar to learners at each school,
thus contextualising the material and making it relevant to learners. For this reason of, each presentation was very different from the others.

Each presentation covered similar basic content. However, the examples used, the degree of focus on topics and the demonstration interaction all varied based on issues that were particular to each target audience. The teacher-oriented campaign implementations were also contextualised by the teachers to some degree, but this was not regulated.

Overall the results showed that personalisation of the material to emphasise each school's pertinent issues increased the probability of associated message adoption. At each school that made a personalisation request, the majority of their learners chose that issue as their poster topic. Schools that had expert presentations or teacher-oriented implementations that reported a large degree of contextualisation maintained or improved their internalisation and participation, while the other schools did not. Thus, the findings of Cycle 2 confirm Lesson 13.

A new issue arose from this finding, however. The level of customisation to education material (done by the researcher) cannot be maintained indefinitely using the current educational delivery model. In this instance, all customisation and contextualisation is implemented mainly by the expert presenter (the researcher). In a campaign with a wide range of contexts (many schools scattered over a large geographical area) the scope of material to be customised for each context is immense. Experts are in short supply and therefore a campaign model that is more practical is required. This issue is the motivation for Lesson 15, that:

**Lesson 15**

*Content creation should take into consideration that the availability of resources, the degree of required contextualisation and degree to which a campaign is adaptable are interdependent characteristics of campaign material*

Future cycles should investigate methods of making campaigns more adaptable while continuing to allow high levels of content contextualisation.
9.6.5 Examine whether a correlation exists between campaign’s content emphasis and the content choices depicted in posters

The final issue of interest in Cycle 2 was whether the amount of material dedicated to or the emphasis placed on material, specific campaign content or messages affected whether a learner adopted the campaign message.

*(C2O7) was to*

“investigate whether the amount of coverage particular content received within the campaign aligns with the degree to which the learners depict the topics in their posters.”

The action taken to meet this objective was to place greater focus on issues which related strongly to the target audience in the expert presentations. The issue of piracy, which had not been adopted by any learners in Cycle 1, was selected by teachers at each school. Cyberbullying was the most consistently named issue by the teachers.

Overall, the aggregated results from all the schools did not show a major shift in topic focus among the learners. This initial result indicated that the focus placed on a topic did not affect its adoption. However, this result was completely accurate as not all schools received expert presentations, the main implementation of the objective.

There was a definite increase in adoption of topics that teachers had selected, and learners felt threatened by, e.g. cyberbullying, among learners from schools that had received the customised expert presentations. This trend was apparent in learners from each school that had had an expert presentation, and in some learners from schools that had had teacher-implemented campaigns. As far as schools where topic adoption had increased, posters demonstrated the learners had internalised the messages to a significant degree (rephrased or full). This indicated that the emphasis of the material and activities did encourage learners to adopt these messages; however, this only occurred in the case of topics that learners had a predisposition to adopt, i.e. the topics they felt threatened by.

There was a continued lack of adoption of topics that were relevant to learners but which the learners were not predisposed to accept. These were topics that in their experience either did not threaten them, or that learners had benefited from. Piracy was adopted least by learners; this continued to be the case even with thorough coverage of the topic in expert presentations. The topic was covered in the same way as topics such as cyberbullying, yet this had little effect. This
suggested that content emphasis could not guarantee message adoption if learners are opposed to the message. This reflection is made in the context of a single or limited amount of exposure to material emphasising the topic. It is possible that long-term exposure to content-specific materials that emphasise the message(s) strongly may have an effect.

Lesson 16, learnt because of these findings, was:

Lesson 16

Campaign resources and activities that place strong emphasis on particular content support and encourage content adoption and internalisation. But exposure to the materials and activities cannot guarantee content and internalisation if the learner is opposed to the content's message.

9.7 Conclusion

In general, this cycle successfully improved upon the results of Cycle 1 SACSAA cybersecurity and safety awareness campaign and competition from 2012. Participation increased significantly. Both primary school and high school learners took part. Several lessons were learnt from of the poster analyse and campaign implementation. Lessons learnt in Cycle 0, Cycle 1 and Cycle 2 will continue to be considered in the following third official campaign iteration.
This chapter presents Cycle 3 of the action research process. Cycle 3 examines the interventions conducted on the SACSAA cybersecurity and cybersafety in 2014. This cycle focused on a formal education curriculum while further contextualising and customising the campaign to meet the target audience’s cybersecurity and cybersafety education needs.

10.1 Introduction

The 2014 campaign was the third official iteration of the SACSAA awareness and education campaign and competition. This iteration aimed to make further adjustments to the campaign and to measure the results based on lessons learnt from the 2013 iteration. This iteration was focused primarily on adjusting the campaign to make it more teacher-oriented and adaptable in its implementation. The following sub-sections identify the issues that were addressed, the planned solutions, and the actual results of the implementation. This iteration is presented according to the layout shown in figure 6.2. This was the fourth iteration of five action research cycles and campaign years that were included in the study. The sections below describe the design, implementation, and results of Cycle 3.

10.2 Problem Identification

In Cycle 2 it was revealed that continuing to address the campaign’s design and implementation issues resulted increased participation in the campaign and competition. The audience was therefore larger. A larger audience combined with a greater variety of implementation procedures and variables resulted in a drop in the percentage of learners internalising the content. However, the feedback was positive, and recommended implementations showed improved results in comparison to Cycle 1. Continuing to address issues such as a lack of formalised pedagogical instruction, the appropriate choice and use of brand symbols had a generally positive educational effect on most of the target audience.

Cycle 3 aimed to build upon the campaign practices of previous cycles. Thus, it continued to address problems identified in the previous campaign cycles, while at the same time addressing issues of interest that were identified in cycle results. The issues of interest for Cycle 3 included:

- the continued need for a more formalised education approach, including more formalised material and increased involvement of educators (Section 10.2.1);
• the continued investigation of the use of effective marketing and procurement of participation agreement from the schools and the learners (Section 10.2.2);
• the continued need to increase the relevance and contextualisation of the campaign and its content in order to enhance learners’ education experience (Section 10.2.3);
• the need to increase the adaptability of the campaign (Section 10.2.4).

Each of the issues of interest introduced in past iterations and Cycle 3’s associated objective to address the issue of interest are briefly discussed below.

### 10.2.1 Establish a more formalised education approach with supporting materials

Cycle 1 and Cycle 2 focused on providing sound pedagogically designed and implemented educational experiences to teach cybersecurity and cybersafety. This resulted in several lessons pertaining to the effective design and implementation of such a campaign. Cycle 3 aimed to continue to confirm the results of Cycle 1 and Cycle 2, while exploring further ways to formalise the education approach. There were two objectives to this issue:

1. **Cycle 3 – Objective 1 (C3O1): Provide further formalised, pedagogically-compliant educational resources**

   Cycle 1 and Cycle 2 provided increasing amounts cybersecurity and cybersafety awareness-raising and education materials and resources. Most learners internalised the content to some degree. Therefore, this material was fulfilling its educational purpose. C3O1 aimed to further enhance existing educational resources and to provide additional resources to improve the implementation and effectiveness of the campaign even further.

   The need for a formal curriculum or lesson plan was noted as an issue of interest arising from Cycle 2’s findings and teacher feedback. Providing a cybersecurity curriculum as an additional resource was to be the main action taken to meet this objective.

2. **Cycle 3 – Objective 2 (C3O2): Enable teachers to provide pedagogically designed, cybersecurity education experiences that can be customised to their implementation context**

   Cycle 1 and Cycle 2 demonstrated that involving teachers in the implementation of the campaigns resulted in:

   • high numbers of learners taking part in the campaign and competition
   • improved levels of internalisation of the content learned by the participants.
These consistent findings, Lesson 7, Lesson 9, Lesson 11, Lesson 13 and Lesson 14, led to the belief that teachers should be empowered to provide cybersecurity education experiences. Klimburg (2012) recommends formalised education. Feedback from teachers indicated that teachers are willing to become more involved, provided they are fully equipped to educate learners effectively about cybersecurity. Providing teachers with a standard, pedagogically designed lesson plan and content that they can customise to meet their learners’ contextual needs should fulfil this objective. Therefore, the inclusion of the proposed curriculum to be implemented as an action to meet C3O1 would meet this C3O2.

Both objectives would be met by examining how providing a formal curriculum and making the campaign more teacher oriented would affect learners’ cybersecurity education experience; this was the general issue of interest.

10.2.2 Examine the effect of method(s) used to gain school participation and gain learners’ attention

The results of Cycle 2 showed that no particularly strong brand identity had been formed for the campaign and its brand symbols. Most learners had not included either the mascot nor the SACSAA logo on their posters. However, the eventual formation of a brand identity remained an issue of interest. Therefore, Cycle 3 continued to investigate the issues of interest from Cycle 1 and Cycle 2 relating to the brand symbols.

Cycle 3 – Objective 3 (C3O3) is to: examine whether the choice of brand symbols included in the educational campaign affects the adoption of these symbols and by extension the formation of part of the campaign’s brand identity. This objective continued the investigation from C2O, examining the practical application of Lesson 10. Cycle 3 intended to include multiple brand symbols. The issue of interest would be whether including both male and female mascots would make the symbols more relevant to the target audience.

Cycle 3 – Objective 3 (C3O3A): is to: consider the impact of the selected brand symbols on the formation of a SACSAA campaign brand identity and its memorability. This continues C2O3A.
10.2.3 Increase the relevance of the campaign and its content for learners

Cycle 2 validated Lesson 13. The findings revealed that highly contextualised and customised material consistently contributed to learners developing and depicting a more personally contextualised understanding of the campaign messages. Cycle 3 continued to validate the findings of Cycle 2 and Lesson 13, and thus the objective of this issue was an extension of C2O6. This included investigating how to empower teachers to make material more relevant to their learners. This additional focus relates to C3O2.

*Cycle 3 – Objective 3 (C3O4) is to: continue to design and implement the campaign and its content in order to contextualise and customise it for the target audience.*

10.2.4 Adapt the campaign to make it more adaptable

Lesson 13 showed that customising and contextualising the campaign and its resource content to suit the needs of the target audience could lead to an increased level of internalisation of the content. This was confirmed in Cycle 2.

Cycle 2 relied on the expert presenter to provide the bulk of the customisation in the expert presentation. However, if the campaign’s target audience were to continue to grow, as is expected, then the level of customisation to education material (by the researcher) could not be maintained indefinitely if the current educational delivery model continued to be used.

In a campaign with a wide range of contexts (many schools over a large geographical area) the scope of material that would eventually require customisation for each context would be immense. Experts are limited, and therefore a more adaptable campaign model was needed. This issue led to the formation of Lesson 15 at the end of Cycle 2.

Lesson 15 states that *content creation should take into consideration that the availability of resources, the degree of required contextualisation and degree to which a campaign is adaptable are interdependent characteristics of campaign material.*

The issue of interest of Cycle 3 was to investigate how to make campaigns more manageable while continuing to allow for high levels of content contextualisation. This issue could be resolved by increasing the role of the education expert and at the same time reducing the role of the
campaign’s subject-matter expert, provided that the educator is equipped with the tools and knowledge to achieve the goal.

*Cycle 3 – Objective 3 (C3O3) is to: investigate how to make the campaign more manageable while continuing to enable high levels of content contextualisation by increasing the roles of teachers in the campaign.*

Section 10.2 presented the problem identification for Cycle 3 of the action research process. The next section will present the plan of action for studying and addressing Cycle 3’s problems.

### 10.3 Action planning

This section outlines the planned implementation for the 2014 iteration of the SACSAA cybersecurity and safety awareness campaign and competition. It describes how the iteration was intended to be implemented in the recommended scenario. This section will be presented according to the outline displayed in figure 10.1.

![Figure 10.1 Cycle 3 action planning section outline](image)

Figure 10.1 Cycle 3 action planning section outline

This section describes how the iteration was intended to be implemented in the recommended scenario.
10.3.1 Target audience

In Cycle 1 and Cycle 2, the target audience had consisted of primary school and high school learners. However, this year it was necessary to refine this focus once again. There are two reasons for this refinement:

1. **Cycle 3 was particularly focused on the use of a resources that primarily targeted primary school learners**
   
   During the 2014 campaign planning sessions a decision was made to include more formalised education in the form of a curriculum (discussed in section 10.2.1). The selected curriculum focused on primary school learners as its target audience. The addition of a formalised curriculum was an issue of interest in Cycle 3 of the campaign. The description of the curriculum and the reasons for its selection are discussed in section 10.3.2.1.1.

2. **High school learners required more engaging and age-appropriate education material**
   
   In Cycle 1 and Cycle 2, all high schools implementing the campaign accepted the printed educational resources, but declined an expert presentation. Based on feedback from teachers the materials had been incorporated into a single information technology lesson and displayed.

   Learners were therefore exposed only to the more generic awareness-raising and education materials, not to customised presentations, examples, or discussions which the expert presentation was designed to deliver. Their posters were based on the printed awareness-raising materials, their own research based on these materials and the topics their teachers may have emphasised as important.

   The high school learners who had taken part in previous years showed some understanding of the material, and high levels of internalisation of the material. Their posters were generic, however, and some contained images which if published would infringe on the original designer’s copyright. The learners needed more exposure to a more active education approach that targeted their age group, in other words, a curriculum. However, such a curriculum would differ significantly from a curriculum for primary school learners.

   Based on these reasons, a decision was made to exclude high school learners from the reported activities. Other campaign activities were planned to target the age group; however, they now fell beyond the scope of the thesis, and are not included in the remaining research cycles.
Several schools were invited to take part in Cycle 3 of the campaign. Five elected to take part in the educational campaign and compete in the poster competition. This was the first campaign that did not include high school learners. Thus, all five participating schools were primary schools. The overall number of schools participating decreased from six in 2013 to five in 2014. However, the number of primary schools taking part increased from one (2012) to four (2013) and now five (2014).

Participating schools are referred to by their anonymised names: School A, B, D, E, and F. This was the third year of participation for School A, the second year for School B and School C and the first year for the remaining schools. Learners from these schools ranged in age from six to 14 years.

The implementation of the campaign at these schools is outlined in section 10.4. The results of the campaign at each of these schools are presented in section 10.5.

### 10.3.2 The Educational Campaign

Cycle 3’s campaign was designed and implemented to follow most of Cycle 2’s procedures. The educational campaign would continue to follow a more formalised format, contain multifaceted educational resources and activities, and be designed according to brain compatible (BCE) principles outlined in Table 6.2. Cycle 3 would continue to refer to brain-compatible principles numerically as in Table 8.1. The relevant BCE principle/s for each awareness resource were listed in their descriptions.

Taking into consideration the issues of interest for this campaign cycle as outlined in section 10.2, this section outlines the components of the educational campaign. Additions and alterations to the education campaign components include:

- Awareness-raising materials (section 10.3.2.1)
- expert presentations (section 10.3.2.2)
- branding (section 10.3.2.3)
- the invitation and management processes (section 10.3.2.4)

These are discussed in the following sections.
10.3.2.1 Awareness-raising Materials

As part of the formalisation of the cybersecurity education campaign, the C3O1 was to “provide further formalised, pedagogically-appropriate educational resources”. The planned awareness-raising materials for inclusion as part of the campaign would therefore include the awareness materials from Cycle 1 and Cycle 2 as well as additional materials.

Several types of awareness-raising materials were designed for inclusion in the campaign. As in Cycle 2’s campaign, this education effort followed BCE principle 1. The campaign aimed to provide a multifaceted education experience that would appeal to many learning styles and provide multiple opportunities for learning. In order to achieve this, access to multiple educational resources was provided. These resources took various formats, including educational activities to teach and reinforce the cybersecurity and -safety content.

The resources (excluding the expert lecture) were to be distributed with the invitations to participate that were to be sent to targeted schools. They were also intended for upload onto the NMMU SACSAA website where they would be downloadable from Cycle 3’s campaign page. A form allowing schools to request an expert presentation for their learners was also added to the page.

Inclusion of materials on the website was intended to provide learners with access to the educational resources at all times. This would mean that learners could use the materials at their own pace. This is an implementation of BCE principle 8. Expert lecture notes and videos were not included on the website; however, a form to request such an event was made available.

The additional educational resources included informative awareness-raising materials, and the option of a formal educational lecture. As in Cycle 1 and 2, these resources were designed following brain-compatible education principles.

All the awareness-raising and education resources from the Cycle 1 and 2 campaigns were reused in this year’s campaign. The previous section discussed the awareness-raising and education resources. This section discusses the new resources and the resources from previous iterations that were updated.

The resources to be reused in Cycle 3 from the previous cycles included:

- the original topic-specific flyers with single security messages (Figure 8.2, section 8.3.2.1.1)
• the cybersecurity “Snakes and Ladders” board game (Figure 8.3, section 8.3.2.1.2)
• and the cybersafety pledge with Cyber Sid (Figure 8.4, section 8.3.2.1.3)
• the cybersafety 101 flyer (Figure 8.5, section 8.3.2.1.4)
• the additional 101 flyers with separate 101 topics (Figure 9.2, section 9.3.2.1.1)
• the most recent NMMU SACSAA calendar

New materials to be included were:

• cybersecurity and safety curriculum (section 10.3.2.1.1, Appendix F)
• Awareness-raising posters featuring past cycles’ competition winners (section 10.3.2.1.2)

Expert presentations would also continue to be offered. Their content would continue to be refined from the previous year’s implementation.

Each of the new and amended materials and campaign components are briefly described below.

**10.3.2.1.1 Cybersecurity Curriculum**

An action that has become necessary to contribute to address C301, C302, C304 and C305 is the campaigns provision of a cybersecurity and safety curriculum to participating schools and teachers. A pedagogically sound curriculum that provided a complete, customisable cybersecurity education experience for various age groups was required. The researcher would have to create a new curriculum or make use of an existing curriculum that met the requirements.

A curriculum created by Von Solms and Von Solms (2014) was selected (Appendix F). This section describes this curriculum and highlights how it met the requirements.

Von Solms and Von Solms (2014) created the video-based Syllabus (curriculum) for Cybersafety for Primary School Learners. This curriculum was designed for two age groups, ages 10 to 12 years and 13 years and older. It comprises several lessons on specific topics prepared for each age group. Some lessons overlap in order to reinforce reiterate particular aspects.

The curriculum makes use of a selection of videos which that are freely available on YouTube. The videos are used as resources in lesson plans and include learning objectives, lesson procedures, discussion points and learning and assessment activities.

From a resource perspective, a total of 24 lesson plans are provided. Each lesson is made up of three pages:
• page 1 is a lesson plan for the teacher
• page 2 is an assessment exercise for the learners
• page 3 is a memorandum for the exercise

The only part of the lesson plan that is intended for distribution to learners is the assessment exercises. Ideally, teachers should print and duplicate these exercises for learners to complete after they have watched the video and discussed the lesson.

The remainder of each lesson plan is not for distribution to learners. This is intended for teachers to use as a guideline when planning a lesson to discuss the material. Teachers are required to contextualise the material, e.g. discussions and additional examples, so that they are relevant to their learners.

The curriculum was not documented as being explicitly designed to follow BCE pedagogy; nevertheless, it follows BCE principles in several ways. This was a major factor in its selection for use. The remainder of this section outlines the ways in which the curriculum is in keeping with the BCE principles in Table 6.2.

• BCE Principle 1
The curriculum includes many multifaceted and multimodal activities that appeal to various learning preferences. Firstly, lessons make use of video resources and teacher lectures that appeal to visual and auditory learners. Secondly, lesson plans include discussions of content, which appeals to auditory and kinaesthetic learners. Finally, lesson plans include a few activities that appeal to kinaesthetic learners. Combined, these lesson components provide a multifaceted experience for the learner.

• BCE Principle 2
The first way the curriculum reflects BCE principles is in the fact that the curriculum makes use primarily of cartoon-based videos with clear cybersafety messages. These videos are typically brief demonstrations and explanations of various cybersecurity or cybersafety issues, accompanied by advice on how to avoid them. The video examples, language and characters are typically designed to appeal to learners and to be appropriate to specific age groups. The videos engage the learners emotionally. Watching a video in class is enjoyable for learners and thus an implementation of BCE Principle 2. Finally, formative feedback during discussions and from marking or completion of the assessment activities also engages learners’ emotions.
• **BCE Principle 3**
Firstly, the characters in the videos and the examples, the metaphors and analogies included in the content are designed to relate to children. Many of the videos link the cybersecurity issue to related real-world issues or experiences that most children are familiar with or aware of. Thus, the videos allow learners to relate new and old principles, building on past learning and experiences. Secondly, a few lessons included that build on previous lesson content by covering the same or related topics. Finally, the discussions provide an opportunity for learners to reflect on what they have learned and to contextualise it for themselves.

• **BCE Principle 4**
Firstly, the explanations of the videos and discussions relate knowledge to pre-existing knowledge, thereby assisting in the formation of “patterns”. Secondly, the lessons plan and the procedure of each lesson are sequentially organised. This promotes the building of patterned knowledge. Finally, the discussions and assessment activities (e.g. reflective, problem solving and critical thinking problems) promote reflective thought and, by extension, knowledge patterning.

• **BCE Principle 5**
Firstly, the topic content is organised in a sequential manner. Lessons that cover the same topic build upon each other. Topics are explained individually and in relation to one another. Secondly, each lesson has objectives that assist in establishing why each concept or activity is covered or carried out. Thirdly, the discussions encourage the learners to consider the content and derive meaning and understanding in both a personal and a global context.

• **BCE Principle 6, Principle 7, Principle 8**
The curriculum includes several lessons on the same topic. Each lesson has various activities to help review material. These activities and the video can be completed and accessed multiple times, at the learner’s or the lesson’s pace. Activities for individuals and class exercises are included. Exercises and assessments provide an opportunity for learners and teachers to reflect on what has been learned and measure what knowledge has been gained. After completing and marking activities, formative feedback can be provided to learners to guide learners through the learning experience. The feedback can assist in identifying learners’ strengths and weaknesses in the particular topic area, and can make suggestions for consideration in future similar or related topic activities.
10.3.2.1.2 Awareness-raising posters featuring winning posters from past cycles

Numerous new awareness-raising posters were included as an additional resource in Cycle 3’s education pack. The posters featured cybersecurity topic-specific messages that aimed to raise learners’ awareness about particular issues. Each poster included a related poster designed by a past campaign cycle winner. Examples of posters are shown in Figure 10.2 and Figure 10.3 below.

Figure 10.2 Past winner’s personal information security awareness poster included in current and future campaigns

Figure 10.3 Past winner’s cyber stranger danger security awareness poster included in future campaigns
These posters aimed to fulfil a purpose similar to that of the topic-specific flyers (figure 8.2, section 8.3.2.1.1) introduced in Cycle 1. The aim of the flyer designs was to attract learners’ attention, communicate the content and illustrate the concepts as much as possible. This was done to increase understanding and to make the posters relevant to learners. The flyers were designed to appeal to all learners; they would, however, be most attractive to learners with a visual learning style (BCE principle 1).

The posters illustrate BCE principles in the following ways:

- the design of the posters made use of colour, text, and images to attract learners’ attention and convey its message. The design appealed to visual learners (BCE principle 1).
- the winners’ posters depicted scenarios they and their peers could understand and relate to (BCE principle 2 and Principle 3). In addition, some learners may have known winners personally.
- the explanations (text) and images (past winning posters) typically related the message to similar concepts that learners would already know, particularly as they would be that same age or older than past winners (BCE principle 3 and BCE principle 4).
- Overall, the posters served as an educational resource as a peripheral visual in an educational environment (BCE Principle 7).

Overall, these posters served as relevant, attention engaging supplementary educational resources.

10.3.2.2 Expert presentations

In this cycle C3O4 was to continue the design and implementation of the campaign and its content and to contextualise and customise the latter for the target audience. Cycle 3 aimed at enabling this objective through the new curriculum. In addition, it continued to meet the objective through the customisation of the expert presentations.

Schools were to be given the option to have a cybersecurity and cybersafety expert visit the school to deliver an educational presentation. This was not compulsory for schools but rather a recommended plan of action. This section describes Cycle 3’s expert presentation. The expert presentations aimed to contribute to meeting C3O1 and C3O4.
Cycle 3 offered a new presentation called “A Cyber Guardian’s guide to exploring Cyberspace”. It involved the Cyber guardians, mascots Cyber Sid and Cyber Sindi, showing learners around cyberspace. Their tour included:

- happy planets –representing beneficial information and activities, i.e. good cyber behaviours, and activities
- sad planets –representing cyber threats and issues.

The guardians would explain how to make sad planets happy and safe, i.e. how to protect oneself or others against the threats.

The presentation made active use of all brand symbols. The logo was included on the materials, and Cyber Sid and Cyber Sindi were used provide tips and demonstrate some of the generic concepts included in all school presentations.

Most of the campaign’s design and implementation details and its focus on BCE principles from Cycle 1 and Cycle 2’s expert presentation were continued (section 8.3.2.2 and section 9.3.2.2).

In an effort to continue and enhance Cycle 2’s expert presentation procedure, presentations in Cycle 3 were customised and contextualised for each school, to an even greater degree than in Cycle 2. The remainder of the section describes how this was achieved.

Firstly, as in Cycle 2, teachers from each school would be asked to specify the topic(s) they believed related most closely to problems faced by their learners. Greater emphasis would be placed on these highlighted topics and on those topics, that were less successful in Cycle 2 e.g. piracy. As a result, each school would receive versions of the talk tailored to make the content relevant to its learners’ context and experiences. This would make the material more engaging and relevant and therefore easier to learn and draw parallels from (BCE principles 1, 3 and 4).

Each version of the talk was accompanied by a customised presentation created in Prezi. The content covered updated information about the various cybersecurity issues covered in previous cycles presentations, the awareness-raising materials, and the competition categories. Presentations could even be tailored to different age-groups (grades) in order to focus on age-appropriate activities and associated cyber threats. Time limits were imposed on the presentation to suit the target audience’s attention span. Junior primary received a 20-minute presentation. Senior primary and other schools received a 30-minute presentation followed by a 10-minute Q&A session.
Secondly, a further enhancement was the inclusion in the presentations of anonymous stories from the schools’ contexts as examples and discussion points. Teachers provided these stories to the expert prior to the presentation and they were included in the talk to increase its relevance to the target audience (BCE principle 2 and BCE principle 3).

Thirdly, when relevant, winning posters from Cycle 1 and Cycle 2 were included as examples. This practice was continued from earlier cycles.

Fourthly, learners were more frequently involved as active participants in the presentations. Learners could volunteer to participate in demonstrations of concepts (acting them out) during the talk. This increased interactivity and engagement by the audience and made the demonstration fun (BCE principles 1, 2 and 7). The Q&A sessions were retained and increased during the presentation (BCE principle 6).

Finally, additional media and sound effects were incorporated into the material to engage learners and attract both their focused and peripheral attention (BCE principle 1 and BCE principle 7). Examples of how this was done included the use of sound effects accompanying good and bad lesson tips and the inclusion of a few select videos from the curriculum as teasers in certain topics.

10.3.2.3 Branding

The branding used in the Cycle 3 campaign was a combination of the SACSAA logo, a redesigned Cyber Sid and a newly introduced Cyber Sindi mascot. Figure 10.4 shows the light blue Cyber Sid on the left and the pink cyber Sindi on the right.

![I am Cyber Aware!](cyberaware.org.za)

Figure 10:4 Redesigned and reintroduced Cyber Sid (left) and newly introduced Cyber Sindi (right)
A consultation with a marketing expert resulted in the inclusion of a new female mascot. The expert recommended that including mascots of both genders would be more inclusive of the target audience. It would allow more learners to relate to the character if they could choose which one they were comfortable with. This recommendation was in keeping with BCE principle 2 as having two mascots appealed to the learner’s emotions and feelings of familiarity. Thus, Cyber Sindi was introduced and Cyber Sid received a makeover to ensure that the mascots were similar.

All the brand symbols were directly introduced and featured in awareness-raising materials and expert presentations. The inclusion of two mascots also was designed to apply BCE principle 1, BCE principle 5 and BCE principle by allowing multiple opportunities for learners to passively and actively view or interact with brand symbols in material and build associations between the mascots and the messages in the content.

Cycle 1 and Cycle 2’s results showed that, in general, there was a very low acceptance of brand symbols, and by extension limited formation of a brand identity among learners. Cyber Sid was the most acknowledged brand symbol and showed some memorability. Objective C3O3 and C3O3A focused on examining the effect of including these new or reinvented brand symbols. This was to be the final investigation of brand symbols, building on Cycle 2’s focus on the SACSAA logo and Cyber Sid.

10.3.2.3.1 Cyber Guardian Awareness Badges

A number of Cyber Guardian Awareness badges were designed and manufactured for inclusion in the education campaign (Figure 10.5). These badges included Cyber Guardian Sid and Cyber Guardian Sindi on separate badges, with the phrase “I am Cyber Aware” and the SACSAA website address. The badges were created to replace the cybersecurity awareness stickers (Figure 8.8, section 8.3.2.3.1) which were introduced in Cycle 1.

Figure 10:5 SACSAA campaign mascot awareness badges
The plan was to use the badges in place of the stickers as an award in the award programme introduced during presentations.

The expert would distribute the badges during school presentations to reward learners who participated actively. Learners who asked questions, answered questions, or helped in other ways during the presentation were all given badges.

The use of the mascot’s image on the badges aimed to continue developing strong visual-verbal (word-picture) associations between the mascots and the campaign messages (BCE principle 5). The wearing of the badges at school would also serve as a repetitive, peripheral reminder of the campaign and its content by enforcing the visual-verbal association (BCE principle 7). The badges might also elicit positive feelings about the campaign and its messages (BCE principle 2).

10.3.2.4 Invitation to participate

The plan for Cycle 3 continued followed Cycle 1 and Cycle 2’s practice in launching the campaign early in the year. The educational part of the campaign ran from April 2014 until the end of October 2014. This was the period during which experts visited schools and conducted presentations. The curriculum could be used by the teachers from the moment they received it. Teachers were free to decide when and how often they would use. The poster competition was open for submissions from 17 October until 21 November 2014. The due date moved from the last week of October (SACSAA Cybersecurity and Safety awareness week) because of a conflict with other activities.

The plan to advertise and encourage participation followed Cycle 2’s implementation. Invitation and resource packs were sent to schools in the metropole via post and e-mail at the very beginning of the campaign. The packs contained:

- a professionally designed advertisement (Appendix D Figure 3)
- the awareness-raising materials (topic-specific awareness-raising flyers (Figure 8.2, section 8.3.2.1.1), cybersecurity snakes and ladders game (Figure 8.3, section 8.3.2.1.2), cybersafety pledge forms (Figure 8.4, section 8.3.2.1.3), the cybersafety 101 flyer (Figure 8.5, section 8.3.2.1.4), the additional 101 flyers (Figure 9.2, section 9.3.2.1.1), a 2015 SACSAA calendar featuring past Cycle winning posters, additional awareness-raising posters featuring past winners’ entries (Figure 10.3, Figure 10.3 and other additional posters) and the cybersecurity and safety curriculum Appendix F)
- a request form (and contact details) for a free expert presentation
• a covering letter explaining the importance of cybersecurity and the campaign, why it was relevant to children and what participation would entail.

The invitation pack was highlighted on the SACSAA website and the resource pack could be requested if schools signed up to enter.

Plans were made to visit schools to speak with the principal or school teachers who would be involved in championing the campaign. This implementation style is supported by Lesson1, Lesson 2, Lesson 8, and Lesson 9.

10.3.3 The Competition

As in Cycle 1 and 2, invitations to participate in the poster competition were included in the educational campaign’s information and resource packages. The overall purpose of the competition didn’t alter from Cycle 2. The competition was part of the educational effort, as well as the method by which the data was gathered about the impact of the campaign on learners.

The implementation of the competition barely altered from 2013 (section 9.3.3). Neither the requirements for poster entries nor its rules changed. The only change was that more prizes were offered. Feedback received from teachers in previous cycles had indicated concern that younger learners (age 6+) were competing with older learners. This year there were different prizes for different age groups. A total of 36 prizes was advertised, for three age groups: 6–8 years, 9–11 years and 12–13.

If the number of participants from schools that had participated in both the 2013 and 2014 campaigns increased; this was possible related to the increase in number of prizes. This will be discussed in section 10.5.3.1

As in previous years, the winning posters would be incorporated into future SACSAA campaign awareness-raising materials and the annual NMMU SACSAA cybersecurity awareness-raising calendar. This served as additional motivation the learners to enter. Feedback from teachers in the past cycles indicated that this motivation was successful as past winners whose work had been featured in materials were vocal about their pride in the achievement and encouraged other learners to participate.

The reflection in the competition of the brain-compatible principles remained unchanged from the description in section 8.33.
10.3.4 Measurements for use in the analysis of the campaign

The success of Cycle 3’s campaign would be evaluated using data gathered from the poster competition. As in the previous two cycles, a qualitative content analysis, as described by Krippendorff (2004), would be carried out on all poster entries. The following questions were asked in the analysis of each poster:

1. How many learners participated? (section 10.3.4.1)
2. What topic(s) is covered by the message(s) in the poster? (section 10.3.4.2)
3. How well has the cybersafety message been internalised (in the researcher’s opinion)? (section 10.3.4.3)
4. Which brand symbols, if any, are present in the posters? (section 10.3.4.4)

The primary reasons for the measurements, and methods, for gathering the measurements remained unchanged from Cycle 1 and Cycle 2 (section 8.3.4 and section 9.3.4). However, some additional reasons are described below.

10.3.4.1 Learner participation

Cycle 3 will continue contextualising material and providing relatable educational resources. An expert will contextualise the presentation for each school and teachers will contextualise the examples and activities in the curriculum. The latter will be available in both recommended and teacher-oriented campaign implementations. In a full-scale campaign, there would be more teachers than experts involved. Therefore, the teachers’ contextualisation and implementation of the curriculum would be the most customised feature of the campaign for most learners. Exposure to this educational experience could result in higher participation numbers from schools where the curriculum is implemented. In Cycle 3 this metric measures whether the number of participants each year is influenced by the addition of the curriculum to the educational resources.

10.3.4.2 Posters per topic

The campaign covered all the topics that have been included since its inception. The emphasis placed on each topic varied, however. This was affected by whether:

- the topic was made particularly relevant to the target audience by the campaign creators (campaign resources content) or by the expert presenter (expert presentation content)
• the teacher(s) had requested that the topic be particularly focused on by the expert presenter
• the teacher(s) themselves had focused on topics while using the curriculum to teach learners.

This measurement was included to see which topics were depicted most often in posters and to identify any changes in topic depiction trends.

In Cycle 3 this measurement will be used to identify which topics are depicted most often in posters. The previous cycle established that quantity of material covering a topic did not necessarily guarantee internalisation of its message (Lesson 16). It did, however, encourage adoption and internalisation of the material if the learners were willing to accept it. This measurement will indicate which topics the learners accept.

10.3.4.3 Internalisation of Cybersecurity or Cybersafety Message

The focus of this measurement in Cycle 3 will be on measuring whether the continued customisation of educational materials and the provision of a teacher-oriented curriculum influences the overall percentage of learners who internalise the material, as well as the percentage of learners per degree of internalisation.

10.3.4.4 Presence of Brand Symbols

Overall, the purpose of this measurement has not altered since Cycle 1. In Cycle 3, this measurement aims to determine whether incorporating a mascot for each gender (Cyber Sid and Cyber Sindi) will result in a mascot or logo being featured more frequently in poster submissions. Inclusion of the mascot could indicate that learners relate to the mascot or associate it with the campaign message.

The percentage of posters featuring brand symbols will then be compared to previous cycles to determine whether a brand identity has been created for the campaign, and to consider the relevance and/or internalisation of these symbols.

Section 10.3 outlined the recommended implementation for the Cycle 3 campaign iteration. The next section describes the actual implementation of the campaign.
10.4 Implementation

This section describes how the campaign was implemented at each school that chose to take part and submit posters. As discussed in the 2012 cycle, implementation at each school was dependent on what the school itself would allow and support. A key decision taken this year was whether schools would make use of the SACSAA cybersecurity and safety curriculum. The curriculum would be incorporated into recommended and teacher-oriented campaign implementations.

In Cycle 3, the school results will be discussed in relation to their implementation choices. Schools that made the same implementation choices were grouped together. This was done to simplify discussion and comparison of the results.

School A’s implementation that followed the recommended implementation of the campaign is discussed first as it forms its own implementation group (section 10.4.1). The implementation of the remaining schools is discussed according to the following implementation categories:

- Recommended implementation (section 10.4.2.1)
- Teacher-oriented implementation (section 10.4.2.2)
- Limited implementation (section 10.4.2.3)

The implementation of the campaign at each school is described below.

10.4.1 School A

Cycle 3 was the third year of participation for School A. The school was asked to take part by personal invitation delivered by a campaign representative at a meeting between the SACSAA representative, the principal and the teachers who would be involved in implementing the campaign. The school once again opted for the recommended version of the campaign. The school therefore:

- accepted the materials
- opted to have an expert address their learners in a guest lecture
- committed to teachers completing the cybersecurity curriculum with their learners
- committed to regularly encouraging the learners to participate in the campaign and competition
Two versions of the expert presentation were presented at the school, to different grade groups. The examples, discussions and other customised features of the expert presentations were adjusted to suit each audience. Some media examples were selected and included to make the presentation more relevant to learners. Different media clips were used for different age groups.

Teachers requested that the customised presentation focus on the issue of cyberbullying in both the junior and senior primary groups because of instances of cyberbullying had occurred at the start of the school.

10.4.2 Other Schools

Three groups of implementation patterns emerged. These are described below.

10.4.2.1 Recommended implementation

This was the second year of consecutive participation for School B and School D. Both schools took part for the first time in Cycle 2. This year, both schools received a postal invitation and a visit from a SACSAA representative. The meetings involved the SACSAA representative, the principal, and the teachers who would be involved in the campaign activities at the school. Both schools opted to follow the recommended campaign implementation the in the same manner as School A.

Teachers from both schools made requests for the expert to customise the presentations so that they focused on the topics of cyberbullying and information and password security. These topics were what School B had requested in Cycle 2, but was for School D a broader customisation request as in the last cycle the school had asked for extra focus on cyberbullying only. School D’s teacher also asked that stranger danger be emphasised, particularly in the context of social networking. This teacher reported that many of the learners were already using social media despite being under age according to the platforms terms of use.

The only other differences between the two campaign implementations related to audience and actions taken by the expert in the customisation of the expert presentation.

As in Cycle 2, School B’s teacher arranged that the whole school would take part in the campaign. Ages of the participants from School B therefore ranged between 6 to and 13 years. School B opted to have two separate presentations, one for junior and one for senior primary learners. This was the same as School A’s implementation. On the other hand, School D continued to focus on
Grade 4 learners, whose ages ranged from 9 to 11 years. A single presentation was conducted as all learners were in the same age group.

Feedback from both schools indicated that they had made use of all the educational resources and successfully completed the cybersecurity curriculum with all participating learners. The teachers indicated that the implementation had been a generally positive educational experience. They indicated that they believed that learners had learned from and internalised the content. Both teachers had noted some changes in cyber behaviour.

10.4.2.2 Teacher-oriented implementation

School E was the only participant in Cycle 3 to follow a teacher-oriented campaign implementation. This was the first year of participation for the school. School E was invited to take part in the campaign and its competition during an introductory visit from a SACSAA representative. The meeting involved the SACSAA representative, the principal, and the teachers who would be involved in the campaign activities at the school.

School E chose to follow the recommended planned procedure for implementation but excluded the expert presentation from the programme. This approach relied primarily on teachers actively championing the material and following the provided curriculum. All contextualisation was done by teachers during reflections on the lesson videos and in discussions on the concepts. Teachers and learners provided examples of scenarios from their own or known experiences, which they believed related to the content.

The teacher exposed all learners from Grade 1 to Grade 7, ages 7 to 13, to the campaign. All learners in attendance at the school therefore received cybersecurity and safety education. However, not all chose to take part in the poster competition.

Feedback from teachers showed that curriculum implementation was recommended. Teachers took learners through all the age-appropriate lessons and provided some contextualisation and customisation of the material, making it more relevant to their learners; teachers indicated that the topic of cyberbullying had been focused on particularly.

10.4.2.3 Limited implementation

School F was a first-time participant. The school received an invitation to participate during a visit from a SACSAA representative. The subsequent meeting included the representative and the
principal; no teachers were in attendance. The school chose to take part but did not want an expert presentation to be delivered to learners. Initially, the school committed to implementing a teacher and curriculum-oriented campaign procedure. It was provided with the educational resources as discussed in section 10.3.2. However, feedback from the teacher on the submission date for posters indicated that only a limited implementation of the campaign had occurred.

Telephonic feedback from the teacher indicated that the curriculum and materials had not been used in any classroom lesson. The campaign’s awareness-raising materials and the competition advertisement had been displayed in a public area in the school. This school’s implementation of the campaign was very like Cycle 0’s implementation of the educational campaign; however, it included a greater number of educational materials. Learners were expected to engage in self-study and to motivate themselves to take part in the campaign.

Reminders about closing date for final submission of posters were sent out via e-mail to all the schools and the teachers concerned, who had been invited or had indicated their intention to participate. The reminders also confirmed the date by which the schools would be notified of winners, and the date for the prize-giving.

Section 10.4 discussed the real-world implementation of the 2014 SACSAA campaign and poster competition at each participating school. The following section presents the results of the campaign and competition.

10.5 Results and Evaluation

This section presents the results of the 2014 SACSAA Educational Campaign and competition. The layout of the chapter is presented in figure 10.6.

It begins by discussing the results from School A (section 10.5.1), and then the results from other schools in Cycle 3’s campaign (10.5.2). The section concludes with a discussion of the general results of the campaign, based on the data from all participants.
This section presents the findings from School A. Measurements from Cycle 3 include: the number of participants from the school, the number of posters depicting each cybersecurity or - safety topic, the degree to which the cybersecurity or cybersafety messages were internalised, and finally the number of posters that included depictions of the campaign mascot or other branding (brand identity). These measurements are discussed in turn below.

10.5.1 School A

This year, the number of learners increased from Cycle 2 (57 learners) to 90 learners (Cycle 3). As a result of a direct request from the researcher, teachers did not select entries for the competition. Any learner who wanted to take part submitted a poster to the campaign.

School A is a school with small class sizes. Each child submitted a poster; 90 posters were received, despite the competition being voluntary.

This 100% participation cannot be conclusively linked to any one component of the campaign. Rather, it is attributable to the entire “package” and process. Feedback from teachers indicated
that learners were attracted to the campaign as a result of their past experience and the expert presentation. This interest was sustained by the curriculum, awareness-raising resources and activities, and the competition.

10.5.1.2 Posters per topic

Figure 10.7 presents the percentage of Cycle 3 posters on each topic. It also provides a comparison with topic coverage in Cycle 1 and Cycle 2.

School A followed the recommended campaign implementation. The teachers requested that the expert presenter focus particularly on cyberbullying. They themselves also placed extra emphasis on this topic during their coverage of the cybersecurity curriculum.

In comparison to Cycle 2’s results, Cycle 3’s poster analysis shows a definite shift in the percentages of posters depicting each topic. The first noticeable shift was that the cyberbullying topic emerged as the most frequent topic in the Cycle 3 posters. Most learners (55.56%, 50 of 90 learners) depicted one or more cyberbullying-related message on their poster. Cycle 3’s result represented a considerable increase over Cycle 2’s 31.58% (18 of 90) and Cycle 1’s 25.53% (24 of 94 learners). While cyberbullying had been one of the most depicted topics in previous cycles, this was the first cycle in which it was most often used by learners. These School A learners were exposed to several education modes that emphasised cyberbullying. Also, they were willing to learn about cyberbullying because of incidents at their school. Together, these factors may have influenced the results. This is a confirmation of Lesson 16.

The second shift in the topic depiction results was visible over multiple topics. There was a general decrease in the percentage of posters depicting all topics excluding cyberbullying and hardware security; most of Cycle 3’s posters illustrated a single campaign topic, that is, cyberbullying.

The third shift was that information and password security was the only topic to show a significant decrease in the percentage of posters in which it appeared. Cycle 3’s result of 18% (16 of 90) of posters featuring the information and password security topic was the lowest rate for this topic at School A, in comparison to Cycle 2 (53%, 30 of 57 learners) and Cycle 1 (49%, 46 of 94 learners). This drop could be the result of the fact that most posters focused on cyberbullying. School A’s campaign also reduced its focus on the topic of personal information disclosure. In Cycle 2, the latter had been a topic that teachers that the expert presenter to focus on.
Figure 10:7 Percentage of School A’s competition posters per topic: Cycle 1 – Cycle 3
10.5.1.3 Internalisation of Cybersecurity or Cybersafety Message

Figure 10.8 shows the degree to which learners internalised the campaign messages they depicted in their competition poster submissions. Overall, results from Cycle 3 revealed that School A’s learners’ levels of internalisation improved over Cycle 2’s results. The levels in Cycle 3 were similar to Cycle 1’s campaign results.

Figure 10.8: How well School A’s learners internalised the cybersecurity or cybersafety messages: Cycle 1 – Cycle 3

The first indication of the improved internalisation rate is that in Cycle 3 there was a definite rise in the percentage of learners who internalised their campaign messages to some degree. This is shown by the decrease in the percentage of un-internalised posters, from 18% (10 of 57 learners) in Cycle 2 to 7% (6 of 90 learners) in Cycle 3.

The second indication that learners at School A were internalising what they had learned to a greater degree was an increase in the number of learners who fully internalised their depicted messages. In Cycle 3 the percentage of such learners increased from 47% (27 of 57 learners) in Cycle 2 to 52% (47 of 90 learners).

An additional finding in Cycle 3 was that posters that reflected internalisation by learners showed signs of the learners having contextualised their understanding of the campaign’s lessons.
These findings show that in the content of School A’s campaign implementation, the use of the curriculum and the customisation of the materials by the expert presenter and teachers had a noticeable, constructive impact on learners’ understanding and internalisation of the campaign concepts.

10.5.1.4 Presence of Brand Symbols

This measurement aims to determine whether the campaign’s brand symbols make the campaign material memorable and relevant to learners. If learners are remembering and featuring the branding symbols in their own posters it may indicate that these symbols are contributing to the development of a brand identity for the campaign in learners’ eyes.

School A’s Cycle 3 competition posters featured the highest percentage thus far of posters containing brand symbols. However, this ranking was not significantly different to Cycle 2’s results. Figure 10.9 shows the percentage of learner posters featuring a single, or a combination of brand symbols in the past three official campaign cycles at School A.

![Graph showing percentage of posters with brand symbols across cycles](image)

Figure 10:9 Percentage of School A’s posters depicting brand symbols: Cycle 1 – Cycle 3

The results for Cycle 3 show that overall there was an increase in the percentage of posters that depicted one or more brand symbols. The percentage of posters without these symbols was greater but had decreased to 68% (61 of 90 learners).
The most popular brand symbol remained the Cyber Sid mascot that had been included in the campaign since Cycle 1. In Cycle 3 it was the most featured mascot, included in 30% (27 of 90) of posters. This represented the highest number of posters yet from School A that featured the mascot.

The newly introduced Cyber Sindi Mascot featured in 10% (9 of 90) posters from School A in this cycle. This was a greater occurrence than the SACSAA logo that been included since Cycle 1 and strongly promoted in Cycle 2. The SACSAA logo was featured in only 6% (5 of 90) of School A’s posters.

These results indicate:

- Learners from School A were more likely to relate to the mascots than the SACSAA logo
- A brand identity for the campaign stemming from the brand symbols was forming in some learners at School A; however, these learners were in the minority.

A brand identity for the campaign will not form in learners’ perceptions instantaneously; however, it seemed to be forming gradually among learners at School A. An issue of interest would be the continued use of the brand symbols in future campaign iterations and their effect (if any) on the formation of a campaign brand identity over time.

This section presented the results of the action research process for School A’s data from Cycle 3. The next section presents this research cycle’s campaign’s results for the other schools that participated in the 2014 SACSAA campaign.

### 10.5.2 Other Schools

This section presents the results of all the participating schools excluding School A. The results are grouped according to schools’ implementation plans (10.4.2). Each school’s results are discussed as part of the implementation group for each measurement.

#### 10.5.2.1 Learner participation

This measurement determined whether the changes made to the campaign had an effect on the number of learners who participated.
10.5.2.1.1 Recommended implementation

This was the second year of participation for School B and School D. In comparison to Cycle 2, both schools had relatively similar levels of participation in Cycle 3 (Table 10.1). School B showed a slight increase in the number of learners, while School D’s participant numbers decreased slightly. Overall, Cycle 3’s campaign implementation did not seem to have made a particular impact learner participation at these schools.

Table 10:1 Number of poster entries from other schools (recommended implementation): Cycle 2 – Cycle 3

<table>
<thead>
<tr>
<th></th>
<th>School B</th>
<th>School D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle 2</td>
<td>102</td>
<td>70</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>109</td>
<td>65</td>
</tr>
</tbody>
</table>

Initially, School D had 68 participants; unfortunately, three learners could not meet the competition’s submission deadline.

10.5.2.1.2 Teacher-oriented implementation

School E was exposed to a teacher-oriented campaign implementation. This was its first year of participation. A total of 44 posters was submitted to the competition. This was a moderate participation rate, but higher than any participation rate at any schools that had been exposed to limited campaign implementation. Therefore, this result supports the supposition that the teachers’ use of the curriculum to educate learners about cybersecurity, and any customisation done to the material during that process, engages learners and encourages them to participate. Feedback from the teacher also indicated that the curriculum:

- engaged the learners
- encouraged learners’ interest in the subject area and how cybersecurity affected them
- combined with the teacher’s encouragement, motivated learners to take part in the campaign’s poster competition.

The overall conclusion was that a teacher-oriented campaign implementation attracted moderate learner participation.
10.5.2.1.3 Limited implementation

School F was exposed to a campaign implementation similar to what was described in Cycle 1. Learner participation was dependent on:

- the learners taking note of the cybersecurity awareness-raising materials and the competition advertisement that were on display at the school
- the learners adopting a self-motivated initiative in engaging in self-study when using the displayed resources
- the learners taking the initiative to submit posters in their own time.

A total of seven poster entries was received from School F. This result was not significant and confirmed the researcher’s belief that the recommended and teacher-oriented campaign implementations were more successful in attracting learner participation and should be encouraged as much as possible.

10.5.2.2 Posters per topic

The schools were exposed to different campaign implementations. Differences included:

- how learners were exposed to the resources
- whether they were exposed an expert presentation
- how much content was emphasised, based on teacher requests or actions
- how the expert presentation and/or cybersecurity curriculum was contextualised and customised.

This measurement indicated how each specific implementation action and experience affected learners’ ability and likelihood of relating to, empathising with, or recalling lessons learnt on the topic(s) depicted in their competition posters.

10.5.2.2.1 Recommended implementation

Both School B and School D requested that cyberbullying and personal information disclosure be emphasised by the expert presenter as topics of relevance to their learners. This request was identical to School B’s Cycle 2 request. However, it was an amended request on the part of School D, which had requested only cyberbullying as a topic of focus in Cycle 2. These requests, as well as the other implementation choices, may have influenced which topics learners were more
inclined to learn and/or depict in their own posters. This section discusses the topic depiction rates for School B and D posters. Figure 10.10 shows the percentage of posters that illustrated each campaign topic for the two schools in Cycle 2 and Cycle 3.

In Cycle 3, the top most depicted topics by both school’s learners were cyberbullying, information and password security and stranger danger. However, the trends in topic depiction percentages between Cycle 2 to Cycle 3’s and the order were very different for the two schools. As the results for the two schools were very different, they are discussed separately.

In Cycle 3, School B’s most depicted topics in descending order were cyberbullying (48%, 52 of 109 learners), information and password security (35%, 38 of 109 learners) and stranger danger (13%, 14 of 109 learners).

It was interesting to note that the top two topics were both customisation requests. These topics were also most frequent in the School B’s Cycle 2 results, but in reverse order. The percentage of posters illustrating cyberbullying lessons increased significantly from 38% (39 of 102) in Cycle 2 to 48% (52 of 109) in Cycle 3. By comparison, the percentage of posters depicting information and password security messages decreased from 43% (44 of 102) in Cycle 2 to 35% (38 of 109) in Cycle 3. Why cyberbullying topics featured more frequently than information and password security topics despite both being strongly highlighted, is dependent on many campaign and learner-related variables.

Result for School B from both cycles support Lesson 16, the emphasis placed by the campaign’s customised and contextualised implementation on topics that learners found relevant resulted in the adoption and depiction of the topics' messages.

In Cycle 3, topics depicted most by learners from School D were, in descending order, information and password security (51%, 33 of 65 learners), cyberbullying (32%, 21 of 65 learners), and stranger danger (32%, 21 of 65 learners). Social networking also featured strongly with 25% (16 of 65) posters depicting messages on this the topic. In comparison to Cycle 2, School D showed an increase in messages from information and password security lessons and a decrease in the cyberbullying lessons. This difference was attributable to the more equal focus on the two topics as a result of the teacher’s customisation requests and actions. The increase in the number social networking topics occurred as many posters linked these three topics to stranger danger. This shift in the results for School D also confirms Lesson 16.
Figure 10:10 Percentage of other schools’ competition posters per topic (recommended implementation): Cycle 2 – Cycle 3
10.5.2.2.2 Curriculum-oriented implementation

This was School E’s first year of participation. The teacher had fully implemented the curriculum and made use of the provided educational resources. The teacher reported placing extra emphasis on the topic of cyberbullying when customising and contextualising lessons and activities. The analysis of posters showed that every topic, excluding piracy and the general browsing and downloading, was featured. The percentage of posters per topic, in descending order was as follows:

- Cyberbullying (57%, 25 of 44 posters)
- Social Networking (32%, 14 of 44 posters)
- Cyber Citizenship (18%, 8 of 44 posters)
- Information and Password Security (16%, 7 of 44 posters)
- Stranger Danger (11%, 5 of 44 posters)
- Cyber Crime, Hardware security and Viruses and Malware (each 5%, 2 of 44 posters)
- Dangers of Online Activities (27%, 1 of 44 posters)

In validation of Lesson 16, the most depicted topic was the one the teacher had focused on most. The next most illustrated topic was social networking, which was strongly associated with cyberbullying, and cyberbullying, also linked to preventing cyberbullying and negative online experiences.

These results suggest that in teacher-oriented campaign implementations, learners tend to focus on topics that the teacher has emphasised.

10.5.2.2.3 Limited Implementation

School F was a first-time participant, had minimal cybersecurity education and only had six participants; the results were of no significance on their own. However, when included in the general results discussion, they do give some indication of which topics the learners at School F were interested in. Posters depicted the following topics:

- Cyberbullying
- Viruses and malware
- Stranger Danger, Social Networking, and Piracy,
It was interesting to note that the topic that learners appeared to relate to most strongly and therefore depicted most often was cyberbullying, much like learners from the other schools and campaign implementations.

**10.5.2.3 Internalisation of Cybersecurity or Cybersafety Message**

This section discusses the outcomes of Cycle 3’s implementation in terms of learner levels of internalisation of the topics.

**10.5.2.3.1 Recommended implementation**

This was the second year that School B and School D had been exposed to the recommended implementation of the education campaign and competition. Figure 10.11 shows the results of the analysis of how well the depicted cybersecurity or cybersafety messages appeared to have been internalised by the learners who created the posters.

![Graph showing internalisation levels](image)

Figure 10:11 How well other schools’ learners internalised the cybersecurity or cybersafety messages (recommended implementation): Cycle 3

In comparison to Cycle 2, School B and School D’s poster analyses in Cycle 3 showed an increase in the overall number of posters featuring internalised cybersecurity lessons, and a decrease in the number that were categorised as being uninternalised. In addition, the percentage of
messages that had been fully internalised increased noticeably for both schools, suggesting that the introduction of the curriculum had contributed to greater numbers of learners understanding and internalising the taught content.

A related observation was that posters, particularly those that had been fully internalised, indicated that the depicted cybersecurity or cybersafety messages had been well contextualised by learners. This suggests that the customisation of the curriculum and education experiences, by both expert presenter and teachers, had had an impact on learners’ internalisation of messages. This was particularly apparent in School B’s posters. The different age groups had been exposed to different degrees of contextualisation of the depicted cybersecurity lessons. Their content was contextualised in much the same manner as the expert presentations and the curriculum had been customised to meet the needs of various age groups. These results from the two schools validate Lesson 13.

10.5.2.3.2 Curriculum-oriented implementation

The results of the analysis of School E’s posters are provided in Figure 10.12. These results showed that the majority of learners internalised the cybersecurity lessons taught by the curriculum and the other educational resources. Only a minority of 15.91% (7 of 44) did not depict their chosen cybersecurity or cybersafety messages or images in a way that could be understood and categorised.

![Figure 10.12](image_url)

Figure 10:12 How well the other schools’ learners internalised the cybersecurity or cybersafety messages (curriculum-oriented implementation): Cycle 3
A finding of interest from School E’s results was that within group of learners who had internalised their depicted messages, there was a difference in the degree to which the material had been internalised. Either they had fully internalised and contextualised the lessons well, or they had only accepted the lesson as it had been presented by the educational material (as given). This trend may have emerged as a result of the extra attention paid to some topics and the cursory coverage of others. Both the results and the feedback from teachers support this theory. The majority of the posters that had been fully internalised dealt with cyberbullying and cyberbullying associated topics. This trend indicates that the messages learners adopted and internalised tended to come from material that was focused on most by teachers.

10.5.2.3.3 Limited Implementation

School F’s posters showed that learners who had engaged in self-study showed an even distribution of depicted cybersecurity or cybersafety messages across the internalisation levels. Two posters were categorised as being in each internalisation position. None of the posters included un-internalised content. No further observations could be made from these data.

10.5.2.4 Presence of Brand Symbols

The presence of brand symbols the posters by learners who were exposed to an implementation of the Cycle 3 campaign was measured.

10.5.2.4.1 Recommended implementation

An analysis of the Cycle 2 and Cycle 3 competition posters showed that none of the learners from School B or School D had included any of the brand symbols on their posters. This result can only indicate that these symbols did not make a significant impression on the learners or their cybersecurity education experience. Therefore, the results from these schools indicate that the inclusion of the brand symbols in material did not contribute to the formation of a brand identity for the cybersecurity education campaign.

10.5.2.4.2 Curriculum-oriented implementation

School E was the only school other than School A to enter posters that featured any of the brand symbols. Only 16% (7 of 44) of submitted posters included a brand symbol, although this was a
greater percentage than all the other schools put together. Both the Cyber Sid and Cyber Sindi mascots were included on posters featuring brand symbols. The SACSAA logo was not depicted on any poster.

The results of this analysis indicate that learners from School E were more likely to relate to the two mascots (characters) than the SACSAA logo. Although these brand symbols had only a marginal presence in the campaign, they had made an impression on some learners and were therefore contributing to the formation of a brand identity for the campaign at School E.

10.5.2.4.3 Limited Orientation

The analysis of the competition posters showed that none of the learners from School F had included any of the brand symbols in their own posters. This result can only indicate that the symbols did not make a significant impression on learners or their cybersecurity education experience. This was to be expected as the only place they encountered the brand symbols was on the campaign advertisement. At School F, the inclusion of the brand symbols in material did contribute to the formation of a brand identity for the cybersecurity education campaign.

This section presented the results of the action research process for Cycle 3 for all schools except School A. The next section will present this research cycle campaign’s general results.

10.5.3 General Results

The schools that participated in Cycle 3s campaign and competition, and which were discussed above, are School A, School B, School D, School E, and School F. This section discusses the general results from the game, examining all the data gathered collectively. The general trends in participation numbers, the number of posters depicting each topic, the degree of internalisation of campaign messages and the presence of brand symbols in posters are investigated discussed.

10.5.3.1 Learner Participation

A total of 314 poster entries was received from the primary school learners from five primary schools. This was the highest number of primary schools to participate since the campaigns first iteration. This year there were repeat participants and new participants. This was the third year of participation for School A (90 learners), the second year for School B (109 learners) and School D (65 learners), and the first year for School E (44 learners) and School F (6 learners).
The total number of entries for the competition dropped from Cycle 2’s record high of 424 entries. In 2013, six schools had taken part, two of which were high schools. This year five schools participated, all primary schools. In Cycle 2 there were high numbers of participants from high schools. This may be related to the schools themselves being large institutions and the teacher’s encouragement. In Cycle 3, the number of schools taking part increased, but the two new schools (School E and School F) were smaller institutions than the high schools in Cycle 2. Even if all learners from the new schools had participated, they would not have been able to match the high school participation rate.

10.5.3.2 Posters per topic

Of the 314 posters submitted, 70% (220 of 314) depicted a single topic and the remaining 29% (94 of 314), multiple topics. The first noticeable trend in the general results was that in Cycle 3 more posters depicted multiple topics than in Cycle 2 (22%, 68 of 424). Many of these posters combined related lessons from the topics, reflecting how learners had internalised a concept. From a general perspective, this was a positive outcome that should be encouraged as it matches the campaign’s overall educational and awareness-raising objectives.

The rest of this section discusses the general trends in preferred and rejected topics, based on the history of the campaign. The results of the analysis of the three official campaign cycle competition posters are reflected in Figure 10.13.

In general, the trend of topic depiction in the whole target audience had not changed. For all three cycles thus far, the overall campaign analysis found that the most depicted topics in descending order were consistently:

- Cyberbullying
- Information and password security
- Stranger danger

Social networking. The least depicted topics were piracy and the browsing and downloading topics. These findings were of interest as both the topics learners showed interest in, and topics they rejected, were topics that were associated and shared several commonalities. In addition, they were topics that were relevant to learners and well covered by the materials. However, learners continued to accept only those messages that reflected their own beliefs.
Figure 10:13 Percentage of all schools’ competition posters per topic: Cycle 1 – Cycle 3
The discussed finding validated Lesson 16 and supported the formation of a sub-lesson, Lesson 16A, which is:

**Lesson 16A**

*Target audiences are more likely to accept cybersecurity lessons that are aligned with their own pre-existing beliefs about the issue or related issues.*

It was interesting to observe that the percentage of posters depicting cyberbullying had increased from cycle to cycle. This may relate to the increased number of schools paying extra attention to this topic. Another trend of interest was that piracy continued to be the most commonly rejected topic, although it there was a very small percentage of posters in which it was depicted in the two most recent cycles.

### 10.5.3.3 Internalisation of Cybersecurity and Cybersafety Message(s)

Figure 10.14 shows the results of the analysis of internalisation of depicted cybersecurity lessons in the target audience. The Cycle 2 and Cycle 3 campaign iterations found similarly high levels of participation. The quantity of data collected was also similar. As a result, their results are more similar than Cycle 1’s results.

![Graph showing internalisation of cybersecurity lessons](image)

**Figure 10.14** How well all the schools’ learners internalised the cybersecurity or cybersafety messages: Cycle 1 – Cycle 3
The analysis shows that from an entire campaign perspective, the percentage of posters depicting internalised (to some degree) campaign lessons was greater in Cycle 3 than in Cycle 2. The percentage of posters that reflected fully internalised campaign lessons was also greater than in Cycle 2. These findings indicate that the inclusion of the curriculum and the delegation of teaching to teachers, in addition to the expert presenter, was exerting a positive effect on the target audience’s internalisation of the campaign lessons and messages. The internalised posters from several schools also reflected higher levels of contextualisation.

10.5.3.4 Presence of Brand Symbols

Figure 10.15 shows the analysis of posters to establish the presence of one or more of the campaign’s brand symbols. Cycle 3’s analysis revealed that the brand symbols continued to be excluded from most posters. However, a finding of interest was that noticeably more posers in Cycle 3 (11%) included brand symbol(s) than in Cycle 2 (4%).

![Percentage of all posters depicting branding symbols: Cycle 1 – Cycle 3](image)

Figure 10:15 Percentage of all posters depicting branding symbols: Cycle 1 – Cycle 3

The most commonly included brand symbol was the Cyber Sid mascot; the least depicted was the SACSAA logo. There was moderate adoption of the Cyber Sindi mascot, enough to account for the differences in the aggregates between Cycle 3 and Cycle 2.
These results led the researcher to two conclusions. Firstly, the mascot (character) brand symbols appear to be more relevant and memorable to the target audience than the SACSAA logo. Secondly, in general, the brand symbols have not yet established a brand identity for the campaign among most of the target audience. Nonetheless, they are slowly beginning to contribute to the establishment of such an identity. An issue of interest would be whether the brand symbols, or a branding identity, becomes more strongly entrenched over time if all the symbols are consistently used in future campaign iterations.

This section presented the general results from Cycle 3 of the action research process for all the schools taking part in the 2014 SACSAA education campaign and poster competition. This concludes the results section for Cycle 3. The next section presents the researcher’s reflections on lessons learnt from this research cycle’s campaign.

10.6 Reflections

This section discusses reflections and lessons learned from the implementation of the SACSAA campaign in 2014. It reports the reflective thoughts and lessons learned from actions taken to address Cycle 3’s issues of interest and their related objectives. These reports are presented in the same order as the objectives introduced in section 10.2. Additional lessons learned in the implementation of the campaign but not specifically related to objectives are presented last.

10.6.1 Establish a more formalised education approach with supporting materials

The first area of interest for Cycle 4 was the continued need for pedagogically grounded and implemented educational experiences about cybersecurity and cybersafety. The first two official campaign iterations had resulted in several lessons pertaining to the effective design and implementation of such a campaign. Cycle 3 aimed to continue to confirm the results of Cycle 1 and Cycle 2, while at the same time exploring further ways to formalise the education approach.

Two objectives were defined in addressing and investigating this issue. The objectives were:

\[ \text{C3O1: “Provide further formalised, pedagogically grounded educational resources”} \]

and
Chapter 10 Cycle 3: 2014

C3O2: “Enable teachers to provide pedagogically designed cybersecurity education experiences that can be customised to their implementation context.”

The action taken to meet both objectives was the inclusion of a formal curriculum in the educational campaign. The curriculum consisted of standard, pedagogically designed lesson plans and content that could be customised by teachers to meet their learners’ contextual needs. The teachers were asked to customise and cover the curriculum with their own students. The results from the Cycle 3 campaign showed that the inclusion and use of the curriculum resulted in more learners internalising the campaign’s content than in Cycle 2. In addition, more learners fully internalised their campaign lessons and messages than in any other cycle.

The actions taken, and the consequent results led to the confirmation of Lesson 7, Lesson 9, Lesson 11, and Lesson 14. Having a teacher (an education expert) make use of a pedagogically designed curriculum and awareness-raising tools to educate learners about cybersecurity was an effective campaign approach. Proof of this effectiveness was that more learners internalised material than in previous cycles and secondly, more learners fully internalised the material.

The campaign’s implementation and its success also inspired a new lesson, Lesson 17:

Lesson 17

A cybersecurity education campaign should enable the continuous education or multiple opportunities for education of the target audience by providing multiple levels of education and relevant resources (scaffolding)

Firstly, the campaign provided awareness materials, which could be used for self-study or supplementary education, as well as access to expert presentations. This raised awareness and helped to teach the learner. Thirdly, the campaign provided a more formal and traditional curriculum. Teachers used this curriculum to educate learners about cybersecurity. This was an initial or additional education opportunity for the learners. Overall, while being exposed to each of these resources, learners were simultaneously exposed to multiple opportunities to learn or reinforce what they had already learned about cybersecurity.
10.6.2 Examine the effect of method(s) used to achieve school participation and gain learners’ attention

The possible formation of a brand identity continued to be an issue of interest this cycle. Cycle 3 continued to investigate branding issues of interest from the previous two cycles. A single objective, with a sub-objective, were outlined to guide the research.

The objective C3O3 was to:

“examine whether the choice of brand symbols included in the educational campaign affects the adoption of the brand symbols and by extension the formation of a brand identity.”

The sub-objective C3O3A was to:

“consider the impact of the selected brand symbols on the formation of a SACSAA campaign brand identity and its memorability.”

The action taken to meet this objective and sub-objective was the inclusion of all past brand symbols (the Cyber Sid mascot and the SACSAA logo) and the introduction of a new brand symbol (Cyber Sindi) in all campaign’s awareness-raising and educational materials and activities. The new brand symbol was included to ensure that mascots representing and appealing to both genders were part of in the campaign. Making use of all the brand symbols was intended to allow equal opportunities for the learners to adopt, relate to and remember them.

The results of Cycle 3 continued to show that the majority of learners had not demonstrated that they remembered, related to, or associated the brand symbol(s) with the campaign. This means that no brand symbol associated, well established brand identity for the campaign had been created among the target audience.

There was, however, some evidence supporting the theory that a brand identity had started to form for some learners. There was a definite increase in the percentage of posters depicting learned cybersecurity or cybersafety messages together with one or more of the brand symbols.

An interesting finding was that the character/mascot brand symbols were depicted more often than the SACSAA logo. This suggests that the mascots were easier to relate to and more memorable for the target audience. This finding reinforces Lesson 10 and is sub-lesson 10A.
This issue of interest will be monitored in future campaign cycles. This will assist in determining whether a brand identity, which associates the symbol (s) and the campaign messages, will continue to form for more learners over time.

**10.6.3 Increase the relevance of the campaign and its content for the learners**

Cycle 3’s activities relating to this issue aimed to confirm Lesson 13. This lesson states that the personalising and contextualising of the campaign and its resources will result in a greater percentage of the target audience internalising the campaign message. Target audience members are also more likely to internalise the material to a greater degree. Cycle 3’s objective to addressing issue C3O was to:

> “continue to design and implement the campaign and its content so that it could be contextualised and customised for the target audience.”

The inclusion and implementation of the curriculum as part of the campaign also contributed to meeting this objective. The curriculum was to be used by the teachers in the context of a particular school or class. The teacher could customise examples, discussions and activities so that they would relate to the target audience. Altogether, the customisation of the learning experiences and content and the involvement of learners’ regular teacher was intended to make the campaign more personal for learners. Increased relevance may contribute to better learning experiences for learners. Better learning experiences in turn can encourage better internalisation of the campaign’s messages. The results of Cycle 3’s poster analysis and the feedback received from teachers indicated that this expectation was met. This finding further confirmed Lesson 13.

**10.6.4 Adapt the campaign to be more manageable**

Cycle 3’s issue of interest was the need to make the campaign more manageable while continuing to enable elevated levels of content contextualisation.

*C3O5 was to:*

> “investigate how to make the campaign more manageable while continuing to enable high levels of content contextualisation by increasing the roles of teachers in the campaign”
The inclusion and implementation of the campaign also contributed to meeting this objective. The use of the curriculum increased the role of the education expert and enabled the elevated levels of customisation to continue. Its implementation may even have allowed higher levels of customisation to occur. Teachers needed to customise their implementation of the campaign to suit their learners’ needs. As teachers were familiar with the audience it was anticipated that they would be able to customise the campaign by using relevant examples and discussions of contextualised versions of campaign issues, something a visiting expert would be unable to do.

Delegating the contextualisation and customisation of education experiences has the benefit of making the campaign more adaptable. It can reach more schools if the main education activities are not the responsibility of the visiting cybersecurity expert. This is because there will always be more teachers available than campaign experts or representatives. This finding builds upon Lesson 11. Making use of existing resources and experts, in this case the teacher, not only makes the campaign more effective by making use of each role-player’s specialised skillset; but it also makes the campaign more sustainable. Applying the lesson allows more role-players to take part in the campaign design and implementation as the need for them arises. A sub-lesson for Lesson 11 is:

Lesson 11A

Making use of existing resources and experts increases a campaign’s adaptability

10.7 Conclusion

Overall Cycle 3 successfully improved upon the results of the Cycle 2 SACSAA cybersecurity and safety awareness campaign and competition. A few positive outcomes occurred, including:

- high levels of participation
- increased percentage of learners from the target audiences internalising the campaign messages
- more learners fully internalising the campaign’s messages
- increased adaptability of the implementation of the SACSAA campaign without compromising the quality of education.
Many lessons were learned from the poster analysis and the campaign implementation. These and the lessons learned in Cycles 0, 1, 2 and 3 will continue to be considered in the fourth official campaign iteration.
11 Action Research Cycle 4: 2015

Chapter 1: Introduction

Chapter 2: Information Security and Cybersecurity

Chapter 3: Information Security and Cybersecurity Education

Chapter 4: Methodology

Chapter 5: Development and Detail about the Selected Issues

Theoretical Basis of Action Research Interventions

Chapter 6: Action Research Process

Cycle 0: Pilot
Cycle 1: 2012
Cycle 2: 2013
Cycle 3: 2014
Cycle 4: 2015

Chapter 7
Chapter 8
Chapter 9
Chapter 10

Chapter 11: Conclusion

Chapter 12
This chapter presents Cycle 4 of the action research process. Cycle 4 examines the interventions conducted on the SACSAA cybersecurity and cybersafety in 2015. This cycle focused on determining whether the message being interpreted by the target audience aligned with the message the educational campaign intended to communicate.

11.1 Cycle 4: 2015

The 2015 iteration of the SACSAA awareness and education campaign and competition was the final fully completed iteration included in this thesis. Like its predecessors, its aim was to improve upon previous iterations’ implementations and results. This iteration only made minor changes to the campaign’s execution, based on the lessons learnt thus far. The focus of the iteration, as described in the next section, shifted to whether the conceptual purpose of the entire campaign: contributing to the fostering of a cybersecurity culture amongst school learners via the education was being met in the way the campaign coordinators had originally envisioned. The following sections provide a detailed discussion of how this was investigated. The iteration is presented according to the layout shown in figure 6.2. This is the fifth iteration of five action research cycles and campaign years covered in this study. The forthcoming sections will describe the design, implementation, and results of Cycle 4.

11.2 Problem Identification

In the past three campaign cycles, the focus was on establishing an education campaign that would educate school learners about cybersecurity. Several lessons were learned in the process. In Cycle 4, the focus shifted from establishing the campaign to determining whether it was fulfilling its intended purpose. Therefore, the two issues of interest were:

- The continued need for a formalised education approach, including formalised education material and the involvement of educators.
- The need to determine whether the audience was interpreting the campaign’ message(s) as the campaign intended them to be interpreted.

Each of these issues of interest and Cycle 4’s associated objective in addressing the issue of interest are briefly discussed below.
11.2.1 The continued need for a formalised education approach, including formalised education material and the involvement of educators

Cycles 1 to Cycle 3 focused on establishing a formalised education campaign approach. This process included investigating the effect of altering or adding components or resources to the campaign. This resulted in campaign results being affected by various changes between Cycle 1 to Cycle 3. The issue of interest for this campaign cycle was the effect that consistency of implementation may have on campaign results. Excluding the expert presentation, Cycle 4’s campaign was intended to be as similar as possible to Cycle 3’s campaign, while taking into account the adaptability of the campaign.

Cycle 4 – Objective 1 (C4O1) is to: “continue to provide formalised, pedagogically sound educational resources”

11.2.2 The need to determine whether the audience is interpreting the campaign message(s) as they are intended to be interpreted

The SACSAA campaign teaches learners the knowledge and skills that will form their fundamental cybersecurity knowledge and skills base. Therefore, it is extremely important that these campaigns communicate their content in a manner that encourages the target audience to receive and interpret it as intended by the campaign’s original content creators.

Up to now, the campaign has focused on raising awareness and educating learners about cybersecurity. However, until this point, there has been no actual measurement to determine whether the overall message being communicated by the campaign is being correctly received by the target audience.

Most awareness-raising campaigns are dependent on the underlying assumption that the audience will not misinterpret the campaign’s message. This is not necessarily true, and such an assumption may lead to undetected miscommunication or misunderstandings occurring between the campaign and its audience. A campaign should have measures in place to check that the audience is receiving the intended message.
Measures must be taken to ensure that deviations from the correct interpretation of the campaign’s intended messages are detected and addressed appropriately within the context of the campaign. Detecting whether the audience’s interpretation deviates from the campaign’s intended result can make it easier to identify adjustments that should be made to the campaign to improve the communication of content for future campaign cycles.

*Cycle 4 – Objective 2 (C4O2) is to: “determine whether the way the target audience is interpreting the message(s) of the campaign material aligns with how the campaign intended them to be understood.”*

Section 11.2 presented the problem identification for Cycle 4 of the action research process. The next section provides the plan of action for studying and addressing Cycle 4’s problems.

### 11.3 Action planning

This section outlines the planned implementation of the 2015 iteration of is presented according to the outline displayed in figure 11.1.

![Figure 11.1](image)

*Figure 11.1 Cycle 4 action planning section outline*

This section describes how the iteration was *intended* to be implemented in this campaign cycle.
11.3.1 Target audience

The age range of the target audience remained unchanged in the 2015 campaign. Cycle 4’s campaign continued to target primary school learners. Several schools were invited to take part in the campaign; all those that were invited, four elected to participate in the educational campaign and compete in the poster competition.

In comparison to Cycle 3, the overall number of participating schools decreased from five primary to four primary schools. School B had planned to participate for a third year (as a fifth school); however, as a result of unforeseen school-related issues it had to withdraw from the competition. School B had maintained a high participation rate, so a marked decline in the overall number of participants in the campaign was anticipated by the researcher.

The schools that chose to participate are referred to by their anonymised names. School A, D, E, and G are primary schools. This was the fourth year of participation for School A, the third year for School D, the second year for School E and the first year of participation for School G.

11.3.2 The Educational Campaign

Cycle 4’s campaign was designed and implemented to follow most of Cycle 3’s campaign procedures. The educational campaign would continue to follow a more formalised format, to offer multifaceted educational resources and activities and to be designed according to the brain compatible (BCE) principles outlined in Table 6.2. Cycle 4 would also refer to these principles numerically as they were listed in Table 6.2. The relevant BCE principle/s would be listed in descriptions of each awareness resource.

Taking into consideration the issues of interest for this campaign cycle, as outlined in section 11.2, this section outlines the components of the educational campaign. Additions and alterations to campaign components included:

- Awareness-raising materials (section 11.3.2.1)
- expert presentations (section 11.3.2.2)
- branding (section 11.3.2.3)
- the invitation (section 11.3.2.4)

These are discussed in the following sections.
11.3.2.1 Awareness-raising Materials

As part of continuing to formalise the cybersecurity education campaign, the C4O1 was to “provide formalised, pedagogically sound educational resources”. The planned awareness materials for inclusion as part of the campaign would therefore include the awareness-raising materials from Cycles 1 to Cycle 3. No new educational resources were planned for inclusion in Cycle 3. Instead, all awareness-raising and education resources from the Cycle 1 to Cycle 3 campaigns were to be re-used in this year’s campaign. The educational resources would include informative awareness-raising materials and the option of a formal educational lecture.

As in Cycles 1 to Cycle 3, the awareness-raising materials and the lecture were designed to follow brain-compatible education principles. This section lists the resources from previous iterations that were to be included in Cycle 4’s campaign implementation.

These were:

- the original topic-specific flyers with single security messages (Figure 8.2, section 8.3.2.1.1)
- the cybersecurity “Snakes and Ladders” board game (Figure 8.3, section 8.3.2.1.2)
- and the cybersafety pledge with Cyber Sid (Figure 8.4, section 8.3.2.1.3)
- the cybersafety 101 flyer (Figure 8.5, section 8.3.2.1.4)
- the additional 101 flyers with separate 101 topics (Figure 9.2, section 9.3.2.1.1)
- the most recent NMMU SACSAA calendar
- cybersecurity and safety curriculum (section 10.3.2.1.1, Appendix F)
- Awareness-raising posters featuring past cycles’ competition winners (section 10.3.2.1.2)

The resources (excluding the expert lecture) were to be distributed with the invitations that were to be sent to targeted schools. They would also be uploaded onto the NMMU SACSAA website where they could be downloadable from Cycle 4’s campaign page. A request form for schools to request an expert presentation was added to the page. These expert presentations were the only altered resource activity to be implemented this year.

11.3.2.2 Expert presentations

In Cycle 4, schools continued to be given the choice to have an expert in the area of cybersecurity visit the school to deliver an educational presentation to learners. This was not compulsory;
nevertheless, it was a recommended plan of action. This section describes Cycle 4’s expert presentation, which aimed to contribute to meeting C4O1.

Cycle 4 presented a new adaption of the SACSAA cybersecurity and cybersafety talk, entitled “The Cyber Guardian’s Cybersecurity Guide”. The majority of the campaign’s design and implementation details and its grounding in BCE principles was taken from Cycle1, Cycle 2 and Cycle 3’s expert presentations (section 8.3.2, section 9.3.2 and section 10.3.2).

There were only a few differences between Cycle 4 and Cycle 3’s implementations. The first was that the material was designed to be more media-centric. The number of video-clips, sound effects and infographics was increased. This was done to make the presentation more visually appealing to attract learners’ attention (BCE principle 1 and BCE principle 7). The second difference was that the customisation of the presentations was less extreme than in Cycle 3, and more similar to Cycle 2’s levels of customisation. This was intended to make presentation at a number of schools more manageable for the expert presenter. Finally, the learners were involved in the presentations to a greater degree than they had been in previous iterations. In this iteration, learners were involved in demonstrating concepts (play-acting) during presentations and in assisting in “real-life” simulations and activities that made the talks more expressive and relevant, and a more engaging learning experience.

The presentation was more demonstration-oriented than earlier cycles.

11.3.2.3 Branding

The branding strategy in Cycle 4 was unaltered from Cycle 3. Future iterations will be used to evaluate whether a brand identity featuring any of the brand symbols will be established. The presence of the brand symbols will continue to be measured for future analysis.

11.3.2.4 Invitation to participate

The plan for Cycle 4 followed the launching practice of Cycles 1 and 2, and the campaign was launched early in the year. The educational part of the campaign ran from February 2015 until 20 July 2015. This was the period during which experts visited schools and conducted expert presentations. The curriculum could be used by the teachers from the moment they received it, and they could use it when and as often as they liked. The poster competition was open for
submissions from 27 April until 26 July 2015. The announcement of the winners occurred at the end of August as a pre-October (SACSAA Cybersecurity and Safety awareness week) event.

The plan to advertise and encourage participation followed Cycle 2 and Cycle 3’s implementation. Invitation and resource packs were sent to schools in the metropole via post and e-mail at the very beginning of the campaign. The packs comprised:

- a professionally designed advertisement (Appendix D Figure 4)
- the awareness-raising materials (topic-specific awareness-raising flyers (Figure 8.2, section 8.3.2.1.1), cybersecurity snakes and ladders game (Figure 8.3, section 8.3.2.1.2), cybersafety pledge forms (Figure 8.4, section 8.3.2.1.3), the cybersafety 101 flyer (Figure 8.5, section 8.3.2.1.4), the additional 101 flyers (Figure 9.2, section 9.3.2.1.1), a 2015 SACSAA calendar featuring past Cycle winning posters, additional awareness-raising posters featuring past winners’ entries (Figure 10.3, Figure 10.3 and other additional posters) and the cybersecurity and safety curriculum Appendix F)
- a request form (and contact details) for a free expert presentation
- a covering letter explaining the importance of cybersecurity and the campaign, why it was relevant to learners and what participation would entail.

The invitation pack was posted on the SACSAA website, and the resource pack could be requested if schools signed up to enter.

Plans were made by the researcher to visit the schools to speak to the principal or school teachers who would be involved in championing the campaign. This implementation style was supported by Lesson1, Lesson 2, Lesson 8, and Lesson 9.

### 11.3.3 The Competition

As in all previous cycles, invitations to participate in the poster competition were included in the educational campaign’s information and resource packages. The overall purpose of the competition did not change in Cycle 4. The competition was part of the educational effort, as well as the method by which the data on the campaign’s impact on learners were gathered.

The implementation of the competition barely changed from 2014 (10.4). The requirements for the poster entries and the rules remained the same. The only change to competition was that more prizes were offered. Cycle 3 had offered a total of 36 prizes for three age groups, namely: 6–8, 9–11 and 12–13 years.
In Cycle 3, the number of participants from most schools increased. This increase in participation may have been related to the number of advertised prizes. Funding this number of prizes proved a challenge, however. Cycle 4’s campaign did not have the resources to continue to offer so many prizes. As a result, prizes were reduced to the “Top 15” posters, regardless of age, as in the 2013 iteration. A drop in participation numbers in the 2014 and 2015 campaigns could possibly be related to the reduction in the number of prizes. This will be discussed further in section 11.5.3.1.

As in previous years, the winning posters would be incorporated into future SACSAA campaign awareness-raising materials and the annual NMMU SACSAA cybersecurity awareness-raising calendar. The potential inclusion of their work in these publications served as potential motivation for learners to enter the competition.

The competition continued to be based on brain-compatible principles remains unchanged from as described in section 11.3.

### 11.3.4 Measurements for use in the analysis of the campaign

The success of Cycle 4’s campaign would be evaluated using the data gathered from the poster competition. As in the previous three cycles, a qualitative content analysis, as described by Krippendorff (2004), would be carried out on all posters. The following questions were asked in each poster’s analysis:

1. How many learners participated? (section 11.3.4.1)
2. What topic(s) is covered by the message(s) in the poster? (section 11.3.4.2)
3. How well has the cybersafety message been internalised (in the researcher’s opinion)? (section 11.3.4.3)
4. Which brand symbols, if any, are present in the poster? (section 11.3.4.4)
5. *In comparison to how the campaign’s messages were intended to be communicated, in what decoding position did the learner’s poster interpretation of the messages fall?* (section 11.3.4.5)

The primary reasons for the measurements and methods of taking the measurements remained unchanged from Cycle 1 to Cycle 3 (section 8.3.4, section 9.3.4 and section 10.3.4). However, some additional reasons for taking these measurements are described below.
11.3.4.1 Learner participation

In Cycle 4, this measurement was gathered to assist in determining whether the consistencies and the minor changes made to the campaign influenced the number of learners taking part in the competition. The consistencies were:

- the same awareness-raising materials were provided;
- this was the second year that the curriculum had been implemented
- all the brand symbols were used in the material and activities.

The differences were:

- the expert presentation was more media- and demonstration-centric than previous campaigns
- levels of contextualisation and customisation were as in Cycle 2 (2013).

Overall, this measurement would indicate whether learner participation remained consistent under the relatively unchanged campaign implementations.

11.3.4.2 Posters per topic

In Cycle 4 this measurement would continue to be used to indicate which topics learners were using most often in their posters. At each school, the implementation of the curriculum and the expert presentation varied according to how it was customised. Either the expert or the teacher would customise the implementation to focus on topics that were relevant to the particular target audience (learners at a particular school). This measurement was not expected to show trends from a general campaign perspective; it might, however, reflect trends at school level.

11.3.4.3 Internalisation of Cybersecurity or Cybersafety Message

The focus of this measurement in Cycle 4 was to measure how the relatively constant campaign implementation and the localised customisation of educational materials (expert presentations and curriculum) had affected the percentage of the learners who had internalised the material to some degree, and the percentage of learners per degree of internalisation.
11.3.4.4 Presence of Brand Symbols

In Cycle 4, the use of brand symbols remained unchanged from Cycle 3. This measurement would indicate whether the consistent use of brand symbols had had any impact on their adoption by learners.

11.3.4.5 Active Audience Theory Decoding position

This measurement relates to C4O2. In order to determine whether a message is being communicated by the campaign, and received and interpreted by the audience in the way it was intended, requires a measurement of some sort. Ideally, the message as it was intended to be sent (the original message) should be compared to the audience member’s interpretation of the communicated message (the interpreted message). Such a comparison would provide valuable feedback that could contribute to the refinement and improvement of the campaign and its approaches.

Several media and communication studies have focused on similar problems. In their field, the media (in various formats) have aimed to disseminate various forms of messages. These messages can be targeted at either very broad or very narrow audiences. One form of media that communicates with its audience in a similar manner to an education campaign is television. Television programmes (factual or fictional) are often intended to convey specific messages and inferred meanings to their audiences.

In the past, programme producers, like some awareness-raising campaign creators, have assumed that the meaning of a programme’s “texts” (messages) were accepted at face value by their audiences (Barker, 2012). However, over time they have come to realise that this is not the case. Instead, television producers and the like have found that audiences may be actively interpreting and producing meaning from the “text” from within their own cultural context. The research area pertaining to this phenomenon has become known as the active audience paradigm. Within this paradigm, there are many theories of how the meaning of the message is communicated and interpreted during the communication process between the “text” creator and the target audience. One prominent model is the Encoding/Decoding model, which was proposed by Stuart Hall (Hall, 1981). Active audience theory and the Encoding/Decoding model were discussed in Section 5.3.
The researcher believes that this model is relevant to this study and could be adapted for use in determining how a cybersecurity awareness-raising campaign’s audience interprets the campaign’s intended message. Determining this interpretation’s decoding positions (section 5.3) could assist in detecting deviations from or uniformity in participants’ interpretations of the meaning of messages, specifically the campaign’s intended meaning.

Active audience theory examines the active, interpretative role of an audience when its members “make meaning” from the media content, based on their own cultural context (Hall, 1981; Munday & Chandler, 2011). This campaign presents the content for each topic using multiple mass media modes including digital media (awareness-raising posters, videos, SACSAA website and online resources, and the curriculum), printed media (awareness-raising posters, informational pamphlets, educational games, the curriculum) and, finally, public events (interactive school visits).

This measurement thus aims to use active audience theory (hereafter “AAT”) as a lens through which to determine whether the SACSAA Cybersecurity Campaigns target audience has unambiguously and uncritically interpreted the meaning of the educational campaign’s awareness-raising themes (messages) as they were intended to be interpreted by the campaign’s creators. Detecting whether audience interpretation differs from campaign intentions may make it easier to identify areas requiring adjustments in future campaigns.

The measurement will be made by categorising learners’ interpretations of campaign messages (shown in their poster submissions) in accordance with one of Hall’s three decoding positions. This categorisation will be assigned depending on whether the poster generally agrees, agrees with minor differences in interpretation, or opposes the campaign’s intended meanings. In the case of posters that show that the audience member did not understand/accept/process the message clearly enough to take any of the above positions, a fourth decoding position, “null” has been added. This additional position is considered necessary as some participants were very young.

In order to determine to which position a poster belonged, the following questions were asked as an evaluation matrix:

1. Does the poster’s textual message support the related campaign topic’s message?
2. Does the poster’s graphical message (examples/warnings) support the related campaign topic’s message?
3. What overall impression (in the researcher’s opinion) does the poster give of the participant’s interpretation of the related campaign topic’s message?

Possible answers to these questions were:

- strongly supports related campaign topic’s message
- partially/vaguely supports related campaign topic’s message with negotiated differences
- opposes related campaign topic’s message
- indeterminable.

If two or more questions were judged as “strongly supporting the related campaign topic’s message”, the poster was classified as having accepted the dominant hegemonic decoding interpretive position. Likewise, if two or more questions were answered as “strongly opposing the related campaign topic’s message”, the poster was classified as having accepted an oppositional coded interpretive position. Other combinations of answers resulted in the poster being classified as having accepted a negotiated coded interpretive position. The only exceptions occurred when two or more questions were answered as “indeterminable”, in which case the posters were classified as having a “null” or “undetermined” position. “Null” position posters were typically considered impossible to interpret without further information. An example of the results of the use of this matrix for classification purposes is shown in Figure 11.2.

An example of a poster that was categorised as accepting the dominant-hegemonic (preferred) encoding/decoding of the campaign’s message for the topic of cyberbullying is shown in figure 11.2a. The text strongly supports prevention of cyberbullying and provided tips on how to do this. The graphics strongly support the message, showing the consequences (emotional pain) of the cyberbullying for the victim and the platforms where this bullying may occur. In general, the poster strongly suggests that the participant agrees with the campaign’s objective of promoting the prevention of ‘cyberbullying and/or falling victim to cyberbullying.

In contrast to figure 11.2a, figure 11.2b shows an example of a poster that was categorised as taking an oppositional coded interpretative position to the cyberbullying topic. The textual message was classified as being oppositional as it did not discourage cyberbullying in any way; instead, it seemed to say that cyberbullying was inevitable, and its consequences should be disregarded. The graphics reflected an example of cyberbullying but did not indicate whether it should be stopped or whether it was undesirable; these were also classified as being oppositional. Overall, the poster seemed to promote cyberbullying rather than discourage it.
This section outlined the recommended implementation of the campaign for Cycle 4. The next section describes the actual implementation of the campaign iteration.

11.4 Implementation

This section describes how the campaign was actually implemented at each school that chose to take part and submit posters. As discussed in the 2012 cycle, implementation at each school was dependent on what the school would allow and support.

The school results from Cycle 4 are discussed in relation to the implementation choices. Schools that made the same implementation choices are grouped together. This was done to simplify the discussion and comparison of the results of schools with similar or different implementation experiences.

School A’s implementation followed the recommended implementation of the campaign and is treated as an implementation group on its own (section 11.4.1). The implementation of the other schools is discussed according to the following implementation categories:

- Recommended implementation (section 11.4.2.1)
- Teacher-oriented implementation (section 11.4.2.2)

The implementation of the campaign at each school is described below.
11.4.1 School A

Cycle 4 was the fourth year of participation for School A. Invitations to participate were delivered to the school by a campaign representative at a meeting between the SACSAA representative, the principal and the teachers who would be involved in implementing the campaign. The school once again opted to follow the recommended version of the campaign. This implementation had not changed its procedure from Cycle 3’s implementation. The school therefore:

- accepted the materials
- opted to have an expert address the learners in a guest lecture
- committed to teachers completing the cybersecurity curriculum with their learners
- committed to encourage learners to take part in the campaign and competition.

Two versions of the expert presentation were presented at the school, one version to each grade group. The examples, discussions and other customised features of these presentations were adjusted to suit each audience. Some media examples were selected and included to make the presentation more relevant to learners. Different media clips were used for the different age groups to ensure that they were age appropriate.

Teachers requested that both customised presentations should focus on the issue of cyberbullying and information and password security.

11.4.2 Other Schools

Two groups of implementation patterns emerged. These are described below.

11.4.2.1 Recommended implementation

This was the third consecutive year of participation for School D and the second for School E. This year both schools received a postal invitation and a visit from a SACSAA representative. The school meetings involved the SACSAA representative, the principal and the teachers who would be involved in the campaign activities at the school. Both schools chose to follow the recommended implementation in the same manner as School A. This was School E’s first year of exposure to the recommended campaign implementation; School E had opted for a teacher-oriented implementation of the campaign in Cycle 3.
School D continued to focus on Grade 4 learners, whose ages ranged from nine to 11 years. School E also continued to target the same audience, i.e. the whole school. A single presentation was delivered as all learners were from the same age group. School E requested a single expert presentation for all learners from Grade 1 to Grade 7. Both schools requested that the topic should be cyberbullying.

Feedback from both teachers indicated that they had completed the relevant curriculum material and activities with their learners. Both indicated that the resources had been easy to use, and the educational experience had been beneficial to their learners.

11.4.2.2 Limited implementation

School G was the only participant in Cycle 4 that followed a limited campaign implementation. This was the first year the school had participated. School G was invited to participate in the campaign and its competition during a visit from a SACSAA representative. The meeting involved the SACSAA representative, the principal and the teachers who would be involved in the campaign activities at the school.

School G initially indicated that it would follow the teacher-oriented campaign implementation approach. That was the recommended procedure but excluded the expert presentation from the programme. This approach relies primarily on teachers championing the material actively and following the provided curriculum. All contextualisation is done by the teachers during the curriculum lessons.

In the event, a limited campaign implementation approach was actually followed. The teacher displayed the provided education resources (including the curriculum lesson plans) on a wall in the Grade 5 (ages 10 to 11) classroom. However, no implementation of the lessons or teacher-driven education occurred. Only a few announcements were made to learners to encourage them to look at the materials on the walls and to take part in the competition. They were expected to engage in self-study using these materials.

Feedback from the teacher concerned confirmed that several learners had read the awareness-raising materials on display.
11.4.2.3 Competition Judging

Reminders about the competition closing date were sent out via e-mail to all schools that had been invited to take part. The reminders confirmed the date by which schools would be notified of the winners and the date of the prize giving.

This section provided the real-world implementation details of the 2015 SACSAA campaign and poster competition at each participating school. The following section presents the results of the campaign and competition.

11.5 Results and Evaluation

This section presents the results of the 2015 SACSAA Educational Campaign and competition. The layout of the chapter is presented in figure 11.3.

![Figure 11.3 Cycle 4 results and evaluation section outline](image)

The section begins by examining the results from School A, followed by a discussion of the results from the other schools that participated in Cycle 4’s campaign. As explained in section 11.4, School A was the only participant in all cycles; thus, its data is discussed separately. The section concludes with a discussion of the general results of the campaign based on data from all participants.
11.5.1 School A

Measurements in Cycle 4 included the number of participants from the school, the number of posters depicting each cybersecurity or -safety topic, the degree to which the cybersecurity or cybersafety messages had been internalised and finally the number of categories of poster from an active audience theory perspective. These measurements are discussed below.

11.5.1.1 Participation

This school had a consistently high participation rate throughout all cycles. Cycle 4 was no different, with the majority (120) of learners at the school taking part in both the campaign and the competition. This was the highest number of participants from School A to date. This could be attributed mainly to increased class sizes and continued interest in the cybersecurity campaign. This result suggested that keeping the Cycle 4 campaign implementation consistent with that of Cycle 3 had not deterred learners from taking part in the campaign in 2015.

11.5.1.2 Posters per topic

Measuring which topics were most and least depicted by learners contributed to an issue of interest in that it was believed that this would indicate the extent to which campaign lessons and topics had been accepted or rejected by learners. Figure 11.4 reflects the results of the analysis. School A was exposed to a recommended campaign implementation. The content covered included the generic materials that were part of the awareness-raising materials and the customised curriculum and expert presentation. As a result of the customisation by both the expert presenter and the teacher, these learners were exposed to learning experiences that emphasised cyberbullying and information and password security lessons more than the other topics. This campaign focus was reflected in learners’ depictions of cybersecurity lesson in their own posters. A few trends were observed.

Firstly, in Cycle 4 the most commonly depicted topics at School A were cyberbullying and information and password security. Cyberbullying was the most depicted topic. This was unchanged from previous cycles even though the percentage of posters depicting cyberbullying lessons (47%, 56 of 120) had decreased slightly (47%, 56 of 120) since Cycle 3 (56%, 50 of 90).
Figure 11:4 Percentage of School A’s competition posters per topic: cycle 1 – Cycle 4
Secondly, the percentage of posters depicting information and password security posters increased from Cycle 3. Cycle 3 was the first cycle in which personal information disclosure was not selected for extra emphasis. Reducing emphasis on the topic resulted in a lower rate of depiction of the topic among learners. The reverse occurred in Cycle 4. This confirmed Lesson 16. Piracy continued to be a neglected topic despite several years of exposure to anti-piracy lessons and campaign messages. This continued to confirm Lesson 16A.

### 11.5.1.3 Internalisation of Cybersecurity or Cybersafety Message

This measurement was intended to determine whether the consistent implementation of the campaign had affected:

- how many learners internalised the campaign’s lessons
- the degree to which learners had internalised the learnt messages.

The consistent implementation of the campaign could have resulted in many of the learners at School A having repeated exposure to similar educational experiences covering similar or identical content to that of earlier campaign cycles. Figure 11.5 shows the results of the analysis of how well School A’s learners internalised the campaign messages in Cycle 4, based on their poster messages and illustrations.

![Figure 11.5 How well School A’s learners internalised the cybersecurity or cybersafety messages: Cycle 1 – Cycle 4](image)

<table>
<thead>
<tr>
<th></th>
<th>As given</th>
<th>Rephrased</th>
<th>Fully</th>
<th>Uninternalised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle 1</td>
<td>14</td>
<td>27</td>
<td>52</td>
<td>7</td>
</tr>
<tr>
<td>Cycle 2</td>
<td>16</td>
<td>19</td>
<td>47</td>
<td>18</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>12</td>
<td>29</td>
<td>52</td>
<td>7</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>14</td>
<td>23</td>
<td>55</td>
<td>8</td>
</tr>
</tbody>
</table>
The first noteworthy result was that, overall, the majority of participants had internalised their depicted cybersecurity or cybersafety message(s) to some degree. In comparison to Cycle 2’s results, the percentage of learners who internalised and did not internalise the depicted messages remained relatively consistent.

The second result worth noting was that the percentage of learners who had fully internalised the information increased. In Cycle 4, School A had the highest percentage of learners who had fully internalised their depicted cybersecurity or cybersafety messages in its history of participation in the competition.

Overall, the results show that in the case of School A, the consistent implementation of the SACSAA campaign had resulted in consistent numbers of learners internalising the campaign messages and rising percentages of learners internalising the material to a greater degree. This therefore had a positive influence on the effects of the campaign.

**11.5.1.4 Presence of Brand Symbols**

This measured the effects of the consistent use of the brand symbols that had been used since Cycle 3 on brand symbol adoption over time. This was measured by whether learners included one or more brand symbol in their own cybersecurity awareness-raising posters. Inclusion would suggest that the learner associated this symbol with the cybersecurity or cybersafety message and/or the campaign. Figure 11.6 shows the results of the analysis in Cycle 4 of School A’s competition posters for the presence of campaign brand symbols.

Cycle 4 produced the highest percentage of posters including brand symbols in the history of the campaign at School A. Although the majority of posters did not include brand symbols, the number of posters that did include them rose. Overall 45% (54 of 120) posters featured one or more brand symbols.

Cyber Sid continued to be the most frequently featured brand symbol (33%, 39 of 120), with the SACSAA logo occurring least (2%, 2 of 120). The Cyber Sindi mascot featured on a several posters, often together with Cyber Sid. Cyber Sindi appeared on more posters in Cycle 4 (19%, 23 of 120) than in the year of her introduction in Cycle 3 (9%, 8 of 90). Overall, the character brand symbols were more frequently depicted by learners than the SACSAA logo.

Generally, the results at School A indicated that the consistent use of the brand symbols in the campaign’s educational materials and activities encouraged their adoption over time. Increasing
numbers of learners appeared to relate to and remember them when exposed to them over time. This was particularly true for the two mascots.

![Figure 11.6 Percentage of School A's posters depicting brand symbols: Cycle 1 – Cycle 4](image)

### 11.5.1.5 Active Audience Theory Decoding position

This analysis determined the learner’s interpretive position as demonstrated in the poster, based on the AAT matrixes (section 11.3.4.5). This measurement contributed to determining whether the audience and the campaign’s interpretation of the meaning of messages coincided or differed. Figure 11.7 shows the results of the analysis conducted on School A’s posters from all four official campaign competitions. Overall, some interesting findings were clear from the results.

Firstly, the results reveal that in every campaign cycle thus far, the majority of learners interpreted the meaning of their lessons from a dominant-hegemonic decoding position. This means that the campaign was effective in its communication of its messages, as the audience interpreted the lessons correctly from the campaign’s perspective.

Secondly, as the campaign’s recommended implementation was altered with the addition of resources, pedagogy and formalised education, the number of learners correctly interpreting the campaign content as it was intended increased. This suggested that the alterations to the campaign had been improvements that had made the campaign more effective in educating learners about cybersecurity. This finding was particularly true for Cycle 3 and Cycle 4.
The percentage of School A's participants interpreting the cybersecurity lesson in the dominant-hegemonic decoding position increased significantly in Cycle 3 when the curriculum was added to the campaign. The results increased from Cycle 2 (65%) to Cycle 3 (78%). Cycle 4 continued this trend, with 80% of participants interpreting their depicted messages in the dominant-hegemonic decoding position.

Figure 11:7 Percentage of School A’s posters per AAT position: Cycle 1 – Cycle 4

Overall, this result indicates that, as far as School A is concerned, the Cycle 3 and Cycle 4 campaign implementation communicated its message effectively to the target audience. There remains room for improvement, but the current campaign can be regarded as an effective educational approach for a primary school learner target audience.

Appendix D Table 2 presents the percentage of School A's posters that were placed in each of the AAT encoding/decoding positions for each topic. The results are shown for all four cycles. These results were included as a matter of interest.

The results from this school for this measurement were published (Reid & Van Niekerk, 2015) and (Reid & Niekerk, 2016).
This section presented the results from School A’s data from Cycle 4 of the action research process. The next section provides the cycle’s results for all the other schools that took part in the 2015 SACSAA campaign.

11.5.2 Other Schools

The other school’s results are grouped according to their implementation details (section 11.4.2). Each school’s results for each measurement are discussed as part of the implementation group.

11.5.2.1 Learner participation

This measurement determined whether the consistent implementation of the campaign had affected the number of learners who took part in the campaign and competition.

11.5.2.1.1 Recommended implementation

The number of participants from Schools D and E increased noticeably in Cycle 4 in comparison to earlier cycles (Table 11.1).

Table 11:1 Number of poster entries from other schools (recommended implementation): Cycle 2 – Cycle 4

<table>
<thead>
<tr>
<th></th>
<th>School D</th>
<th>School E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle 2</td>
<td>70</td>
<td>0</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>65</td>
<td>44</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>77</td>
<td>64</td>
</tr>
</tbody>
</table>

In its third year of participation, School D experienced its highest level of participation thus far with 77 learners submitting posters. This was a significant increase in participation. This school’s learners had been exposed to the recommended implementation of the campaign in previous cycles. This result, combined with the results of past campaigns suggested that the consistent campaign implementation procedure had contributed to attracting more participants.

This was the second year of participation for School E. Previously, this school had adopted a teacher-oriented campaign implementation; this was thus the first cycle in which learners had been exposed to a recommended campaign implementation. The number of participants increased from 44 (Cycle 2) to 64 (Cycle 3). This suggests that the recommended implementation of the campaign, which provides multiple opportunities for learning (Lesson 17), was more
effective in attracting participation than a teacher-oriented implementation. This may be because of the added novelty of the expert presenters as well as the increased number of opportunities for learning and reinforcement of learning about cybersecurity.

Overall, the results from both schools that followed a recommended campaign implementation appeared to indicate that the current procedure and format had attracted and encouraged learners to participate in the campaign and the competition.

11.5.2.1.2 Limited implementation

This was the first year of participation for School G, and the school followed a limited implementation. The teachers encouraged learners to engage in self-study using the campaign’s educational materials. There were only seven competition participants from School G, although teachers indicated that more students had read the awareness-raising materials. This result indicates that, as in Cycle 1 and every other minimal campaign implementation, self-motivated self-study is not the most effective way reaching this young target audience.

11.5.2.2 Posters per topic

The schools were exposed to different implementations of the campaign. Differences included:

- how learners were exposed to the provided resources
- whether they were exposed to an expert presentation
- how much the content was emphasised, based on teacher requests or actions
- how the expert presentation and/or cybersecurity curriculum was contextualised and customised.

This measurement reveals how the actions of each specific implementation and experience affected learners’ ability and likelihood of relating to, empathising with, or recalling lessons learnt on the topic(s) depicted in their competition posters.

11.5.2.2.1 Recommended implementation

Both School D and School E’s learners were exposed to a recommended implementation of the campaign, which was customised to place extra emphasis on the topic of cyberbullying. Figure 11.8 shows the percentage of posters illustrating lessons from each topic in each cycle for School D and School E.
Figure 11:8 Percentage of other schools’ competition posters per topic (recommended implementation): Cycle 2 – Cycle 4
At both schools, cyberbullying, information and security and stranger danger were the most commonly used topics, with cyberbullying the most frequent overall. These results continued a trend that had emerged over the last few campaign cycles. This was a validation of Lesson 16 and 16A. On the other hand, piracy continued to be ignored in posters.

In comparison to Cycle 3, there were no major changes in the percentage of posters depicting the various topics. This result suggests that the current format and procedure of the campaign may have consistently positive results. Future campaign cycles should continue to make use of and refine this campaign procedure.

### 11.5.2.2.2 Limited implementation

School G’s learners were expected to inform themselves using the provided awareness-raising materials. They were only exposed to the material and not any additional or customised activities that placed particular emphasis on a topic.

Of the seven posters submitted by School G, 85.71% depicted cyberbullying lessons and 14.79% depicted Information and password security (personal information disclosure) lessons.

These findings were not significant. However, they were of interest as these were topics that learners related to most strongly. They were also topics that learners had depicted and related to most in previous campaign implementations.

### 11.5.2.3 Internalisation of Cybersecurity or Cybersafety Message

This section briefly discusses the results of learners’ level of internalisation of topics in Cycle 4.

#### 11.5.2.3.1 Recommended implementation

Figure 11.9 shows the results of the poster analysis to determine internalised by the learners of depicted cybersecurity lessons.

Both School D and School E produced results indicating that the percentage of participants who had internalised the depicted cybersecurity lesson(s) had remained relatively constant. In addition, both sets of results showed that the degree to which learners had internalised the cybersecurity lesson had improved since Cycle 3.
In School D, the number of learners who had fully internalised the messages increased in Cycle 4 (64%, 49 of 77) from Cycle 3 (60%, 54 of 65 learners). This was the highest percentage of learners to have fully internalised the cybersecurity lessons at School D thus far.

The number of learners from School E who had rephrased the internalised messages increased from Cycle 3 (19%, 8 of 44) to Cycle 4 (22%, 14 of 64 learners). The number of students who merely accepted the message and internalised it as it was given decreased in Cycle 4 (11%, 7 of 44 learners) from Cycle 3 (41%, 18 of 44).

![Bar chart showing internalisation levels of school posters](image)

**Figure 11.9** How well other schools’ learners internalised the cybersecurity or cybersafety messages (recommended implementation): Cycle 2 – Cycle 4

Overall, both sets of results showed that exposure to the recommended implementation of the current campaign had a relatively consistent educational impact on the target audience.

### 11.5.2.3.2 Limited implementation

The results of the analysis of posters by learners from School G were not significant; however, they are included in the overall campaigns results.

Of the seven posters submitted, 86% (6 of 7) were fully internalised and 14% (1 of 7) included cybersecurity lessons that had been internalised to the level of being rephrased by the learner.
Overall, these results appeared to indicate that the awareness-raising materials provided by the campaign were effective educational tools that could contribute to learners’ internalisation of cybersecurity campaign content. This validates Lesson 7.

11.5.2.4 Presence of Brand Symbols

This measurement examines the presence of brand symbols in posters submitted in the Cycle 4 campaign.

11.5.2.4.1 Recommended implementation

Figure 11.10 shows the results of the analysis of School D and School E’s poster submissions. The results are very different for the two campaign implementations.

![Bar chart showing the percentage of posters depicting brand symbols](chart.png)

Figure 11:10 Percentage of other schools’ posters depicting brand symbols (recommended implementation): Cycle 2 – Cycle 4

School D had been exposed to the recommended implementation of the SACSAA campaign from the outset. Therefore, in the three cycles learners had consistently been exposed to all the brand symbols in various implementation formats. However, learners from School D had never included
these symbols in their poster submissions. This suggests that did not relate relating to or remember the brand symbols well enough to include them in their own internalisation of the campaign’s cybersecurity or cybersafety messages. This would suggest that consistent exposure to a brand symbol will not necessarily result in its adoption, unless a learner relates to it sufficiently.

On the other hand, School E’s results showed that a larger number of learners had adopted the brand symbols in Cycle 4’s (28%, 18 of 64) competition when compared to Cycle 3 (16%, 7 of 44). School E had been exposed to Cycle 3 and Cycle 4’s campaigns, that is, campaigns that made use of all brand symbols. In Cycle 3, learners were exposed to a teacher-oriented campaign and in Cycle 4 to a recommended campaign. The expert presentations were a significant promoter and user of the brand symbols and used them in active branding related activities. Therefore, in Cycle 3 learners were exposed only to the passive presence of the brand symbols, but in Cycle 4 they were actively alerted to their presence. School E’s results suggest that consistent and increased exposure to the campaign’s brand will result in an increased number of learners adopting and including these in their interpretation and memory of the campaign’s cybersecurity or cybersafety messages.

A finding of interest was that only the mascots, Cyber Sid and Cyber Sindi, were included in learners’ posters. This finding continued a trend that was observed in the results from several schools, that is that the character brand symbols appeared to be more successful in capturing a primary school target audience’s imagination than the SACSAA logo.

11.5.2.4.2 Limited implementation

This was School G’s first year of exposure to the branding and the campaign. This exposure was entirely passive, resulting only from reading the printed awareness-raising materials. Of the submitted posters, 71% (5 of 7) included both the Cyber Sid and Cyber Sindi mascots. The remaining 29%(2 of 7) posters contained no brand symbols. Overall, this result corroborates the finding from other schools, that learners related more to the mascots than the SACSAA logo. No further analysis was conducted.

11.5.2.5 Active Audience Theory Decoding position

This analyses the interpretive positions reflected in the posters, based on the AAT matrixes (section 11.3.4.5).
11.5.2.5.1 Recommended implementation

Figure 11.11 reflects the results of the analysis conducted on School D and School E's posters over the past four official campaign competitions. These results indicate that in general the campaign had communicated its content effectively to the target audience. However, there were some trends observed in differences between the campaign cycles at various schools. These differences were more than likely attributable to the contextual differences of the campaign’s implementation at each school. Therefore, the remainder of this section focuses on individual schools’ AAT decoding positions.

![Bar chart showing percentage of other school's posters per AAT encoding/decoding position (recommended implementation): Cycle 2 – Cycle 4]

School D’s campaign and audience was defined as being similar to that of School A. However, based on the results of this analysis, there were definite contextual differences. As at School A, the majority of learners from School D decoded the campaign’s content from the dominant-hegemonic position in every cycle in which the school participated. However, unlike School A, first cycle of participation (Cycle 2) resulted in the most desirable audience decoding position ratio (80% dominant-hegemonic), but this decreased over the following cycles. Over this same period the lowest measurement for oppositional decoding (11%) was reduced to 3%. Generally, there
was an increase in the number of posters that demonstrated negotiated decoding of the messages.

These results suggested that the campaign had been effective. However, it also appeared that when the curriculum was included as part of the campaign and teachers became more responsible for educating the learners, the degree of negotiated decoding increased. This could indicate a need to investigate:

- methods to ensure that teachers are implementing the campaign correctly
- whether teachers’ contextual customisation of the campaign is relevant and in line with the campaign’s content.

Appendix D Table 3 presents the percentage of School D’s posters from Cycle 2 to Cycle 4 that were classified in each AAT encoding/decoding position for each topic. These results included as a matter of interest only.

School E’s results showed that learners had maintained a relatively steady interpretation position in both Cycle 3 and Cycle 4. This may be the result of the implementation having been consistent in the two cycles. The majority of learners from School E decoded the campaign lessons from the dominant-hegemonic position. The percentage increased slightly from Cycle 3 (77%) to Cycle 4 (78%). Simultaneously, the number of oppositional decodings also decreased from Cycle 3 (7%) to Cycle 4 (5%). Overall, these results suggest that the campaign at School E had communicated the content effectively to the target audience, with the latter making only minor changes in their interpretation of meaning of messages.

Appendix D Table 4 presents the percentage of School E’s posters that were decoded in each AAT encoding/decoding position for each topic. The results are shown for both cycles in which the School E participated (Cycle 3 and Cycle 4). These results were included as a matter of interest.

Overall, both sets of results suggest that the campaign was educating the target audience effectively about cybersecurity. There was still room for improvement, but the majority of the target audience appeared to be able to interpret the campaign message in the manner in which it was intended to be understood.
Overall, School G’s posters (100%, 7 of 7) displayed dominant-hegemonic decoding of the campaign’s messages. This suggests that the campaign’s awareness and educational material was effective in communicating the cybersecurity lessons to School G learner’s. This dataset was not large enough to allow any additional observations.

The only topics covered by School G’s posters were cyberbullying and information and password security. In School G’s topic specific analysis both topics were decoded from a dominant-hegemonic decoding position.

This section presented the results from Cycle 4 of the action research process for all schools, except School A, which took part in the 2015 SACSAA education campaign and poster competition. The next section presents this research cycle’s general results.

### 11.5.3 General Results

The schools participating in Cycle 4’s campaign and competition, discussed above, were School A, D, E and G. This section discusses the general results from the game, examining all the data gathered together. The general trends in participation numbers, the number of posters depicting each topic, the general trend of the degree of internalisation of campaign messages and the presence of brand symbols in the posters are discussed.

#### 11.5.3.1 Participation

A total of 268 poster entries was received from the participating primary school learners. This was fewer entries than in Cycle 3. This was probably because there was one less school taking part, and particularly since this was School B that had been a strong participant in previous years.

Despite the overall tally of posters decreasing, the trend of repeat entries was positive. This was the fourth year of participation for School A (120 learners), the third year for School D (77 learners) and the second year for School E (64 learners). All three of these schools showed an increase in the number of participants compared to previous years. In addition, all schools had the highest level of participation since they had begun participating. School G was a first-year participant and had seven participants.
The participation rate for the overall campaign indicated that the consistent implementation of the campaign and its established procedure did not deter learners from participating and participation rates had continued to improve.

11.5.3.2 Posters per topic

Of the 268 posters submitted, 80% (214 of 268) depicted a single topic, with the remaining 20% (54 of 268) depicting two or more topics. Figure 11.12 shows the percentage of posters depicting each lesson each cycle. It also provides a comparison of results from Cycle 4 and those of the other three cycles. In general, the trends in use of topics in posters continued in Cycle 4.

In descending order of percentages, the most frequent topics were:

- Cyberbullying (46%)
- Information and password security (28%)
- Stranger danger (15%)

These were the same topics which were most frequent in every other campaign cycle. The least frequently featured topic continued to be piracy (0%). Over the entire implementation of the SACSAA campaign, the order of frequency of featured topics remained unchanged.

Overall, there are definite trends in the topics to which learners related and adopted or rejected in every cycle of the campaign. Results from Cycle 4 revealed that although there were some minor shifts in the number of posters depicting each topic on a school to school basis, the topics that were accepted and rejected did not change. This occurred despite changes to campaign implementation. This finding validates Lesson 16 and sub-lesson 16A.
Figure 11:12 Percentage of all schools’ posters per topic: Cycle 1 – Cycle 4
11.5.3.3 Internalisation of Cybersecurity or Cybersafety Message

Figure 11.13 shows the results of the evaluation of whether the consistent implementation of the SACSAA campaign affected numbers of learners who internalised the campaign’s content and the degree to which learners internalised their depicted cybersecurity lessons.

Overall, the percentage of learners who internalised their posters’ messages remained relatively constant. Only 10% of the posters depicted cybersecurity content and messages that did not show internalisation of the concepts and/or could not be classified as having been internalised.

In terms of the degree to which the campaign’s messages had been internalised, the results suggested that there had been an improved degree of internalisation. The results showed that while the overall number of learners internalising the campaign’s messages had remained consistent, the number of learners fully internalising the messages had increased. The percentage increased from Cycle 3 (53%) to Cycle 4 (58%).

The findings from Cycle 4 suggest that repeated exposure to the campaign reinforces the cybersecurity lessons and taught concepts and encourages learners to consider and internalise them. This finding leads to the formation of the following sub-lesson to Lesson 17:
11.5.3.4 Presence of Brand Symbols

This measurement evaluated whether the consistent use of the brand symbols in consecutive campaign cycles would affect how many learners incorporated the figure(s) in their own awareness-raising posters (Figure 11.14).

![Figure 11.14 Percentage of all schools' posters depicting brand symbols: Cycle 1 – Cycle 4](image)

In comparison to previous campaign cycles, Cycle 4 had the highest number of posters including one or more brand symbols. Although the majority of learners did not adopt these symbols, 28% did incorporate campaign branding. This result was the highest figure yet in this category and suggests that consistent exposure to brand symbols may result in their adoption over time. This would occur if learners begin to associate the presence of brand symbols in material and activities
with the campaign’s cybersecurity content. This led to the formation of a new sub-lesson in Lesson 10 namely that:

**Lesson 10B**

*The adoption of brand symbols by the target audience is affected by how consistently a brand is incorporated in learning experiences, as well as how frequently the learners are exposed to the brand symbols.*

A trend of interest in this measurement was that the mascots (Cyber Sid and Cyber Sindi) were consistently depicted more often than the SACSAA logo in every cycle of the campaign. This suggests that this the type of brand symbol is more relevant and memorable to primary school learners than a more formal brand logo. This finding validates *Lesson 10 and sub-lesson 10A.*

**11.5.3.5 Active Audience Theory Decoding position**

Figure 11.15 shows the results of the analysis conducted on all the participants’ campaign posters from the past four official campaign competitions. These results include every school that ever participated regardless of the type of campaign implementation it followed. Therefore, these results represent the total number of participants and a mixed range of campaign implementations.

![Figure 11.15 Percentage of all school's posters per AAT encoding/decoding position: Cycle 1 – Cycle 4](image-url)
The results show that the campaign managed to consistently communicate its content to at least 70% of the target audience in each cycle. Each cycle varied in the exact percentage, but the majority of learners were judged to have interpreted the campaign’s messages in a way that was consistent with the meaning the campaign intended to convey. The detailed breakdown of the analysis of decoding each topic is included in Appendix D Table 8. Future campaigns should continue to enhance this effective communication of campaign messages. This measurement will be retained to assist in determining whether alterations made to the campaign affect the audience’s interpretation of campaign messages.

This section presented the overall results from Cycle 4 of the action research process for all the schools participating in the 2015 SACSAA education campaign and poster competition. This concludes the results section for Cycle 4. The next section presents the researcher’s reflections on lessons learnt from this research cycle’s campaign.

11.6 Reflections

This section discusses Cycle 3’s reflections and lessons learned from the implementation of the SACSAA campaign in 2014. This section first reports the reflective thoughts and lessons learned as a result of actions taken to meet Cycle 4’s issues of interest and their related objectives. The reports are presented in the same order as the objectives that were introduced in section 11.2.

11.6.1 The continued need for a formalised education approach, including formalised education material and the involvement of educators

This issue led to amendments, improvements and manipulation of various campaign components, resources, and activities in every campaign since 2011. Cycle 4 aimed to investigate whether simply implementing the campaign consistently would have on the target audience’s learning experience.

C4O1 was to:

“continue to provide formalised, pedagogically-grounded educational resources.”
The action taken to meet this objective was the implementation of the Cycle 3 version of the SACSAA campaign with slight changes and updates. The Cycle 3 campaign implementation was used as it was the most successful at that point.

Overall, the results of Cycle 4 showed that the consistent implementation of the campaign had a positive effect on learners’ educational experience and campaign results. The most notable effect was that, in comparison to previous campaign cycles more learners internalised the campaign messages to a greater degree of understanding. This was the culmination of all the efforts made to meet the target audience’s need for cybersecurity knowledge and awareness.

11.6.2 The need to determine whether the audience is interpreting campaign message(s) as intended

Most awareness campaigns are dependent on the underlying assumption that the audience will not misinterpret its messages. This is not necessarily true. This assumption may lead to undetected miscommunications or misunderstandings occurring between the campaign and its audience. A campaign should have measures in place to check that the audience is receiving the intended message. This was the main issue of interest in Cycle 4.

C4O2 was to:

“determine whether the way the target audience is interpreting the messages of the campaign material aligns with how the campaign intended them to be understood.”

The action taken to meet this objective was the analysis of the campaign’s poster competition submissions using the lens of active audience theory. This theory was used to determine whether learners were interpreting the campaign’s messages in a manner which corresponded with how the campaign intended the messages to be interpreted. The results showed that the campaign had consistently managed to communicate its messages in such a way that at least 70% of the audience had interpreted them appropriately.

Taking into consideration the continued need to measure whether future campaigns are educating the target audience effectively about cybersecurity, a final lesson was outlined. Lesson 18 is that:
Lesson 18

Measures must be in place to enable the evaluation of whether the campaign is communicating effectively with the target audience and thereby meeting the campaign’s educational objectives.

11.7 Conclusion

This chapter presented the general results from Cycle 4. It also concluded the discussion of the SACSAA campaign implementation carried out during the research process reported on in this thesis. The cycle resulted in the identification of two sub-lessons to previously identified actionable knowledge lessons (sub-lesson 10B and sub-lesson 17A) and one new lesson (Lesson 18). Many of the other lessons were also reconfirmed. Overall this was the last campaign cycle to be included in the action research process presented in this thesis. A summary of the actionable knowledge (lessons learned) is presented in Chapter 12.
12 Conclusion

“Beginning in itself has no value, it is an end which makes beginning meaningful, we must end what we begun.”

~ Amit Kalantri
This chapter concludes the thesis. Its purpose is to provide a reflective discussion of the findings of this study. It discusses the relationships between findings and research questions and objectives and it outlines the implications of these findings. It concludes by outlining future, related research opportunities.

12.1 Introduction

Cyberspace is the “complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form” (ISO/IEC 27032, 2012). Cyberspace is an integral part of modern society. It is a highly effective tool and enabler of activities. Cyberspace influences, or is integrated in, all facets of most people’s daily lives and digitally transposed activities. The information, ICT, activities, and users it affects are all assets of importance to organisations or individuals in society. Unfortunately, as with any asset, these are often faced with threats. Threats to users, information and related assets now exist to exploit ICT and ICT users in one way or another for their own purposes. Therefore, a cybersecurity and cybersafety solution is necessary for the protection of cyberspace, and all assets and activities it affects, against potential threats.

Human beings play a significant role in the design, implementation and management of an entire cybersecurity and security process and, therefore, they have responsibilities in this regard. Although processes and technologies can be made theoretically secure, how truly secure they are is dependent on the people involved in their use and implementation. The effectiveness of any information security or cybersecurity and security solutions in the organisational or private context is dependent on the human beings involved in the process. Accordingly, if these human beings are unaware or ignorant of their roles in the security solution they become the weak link in the information security or cybersecurity and cybersafety solution. It is thus essential that all users are educated to combat any threats to cybersecurity and cybersafety.

Children are a particularly vulnerable sub-group within a societal target audience. They are growing up as digital natives who do not necessarily know how to be cyber secure or cybersafe. Added to this, their guardians and teachers may not be monitoring children’s online activities or have the requisite knowledge and experience to teach children to secure their information and protect themselves online. These children therefore require cybersecurity and cybersafety education. Very little literature addresses cybersecurity education for school children, however.
The aim of this study was to address this lack of guidance available for cybersecurity and cybersafety education campaigns targeting school learners by generating actionable knowledge, which would offer guidance for designing and implementing education campaigns that educate school learners about cybersecurity and cybersafety.

12.2 Summary of Lessons Learnt

This section briefly outlines the lessons that were learned from Cycle 0 to Cycle 4 of the action research process. As a result of the requirements of action research, each of these lessons and their implications were discussed in the discussion of each cycle. For this reason, this section only lists the key message of each lesson. For more detail, the reader should refer to discussion in the section where the lesson was introduced. For convenience, these sections are listed next to each lesson. The lessons learned during the past five campaign iterations, the piloted “unofficial” campaign and the four official campaign cycles, are included. These lessons are listed in the order they were learned, as discussed in previous sections. The sub-lessons learned at various stages are presented under their parent lesson.

The lessons which were originally learned in Cycle 0 and which were reconfirmed over the course of consecutive cycles included, Lessons 1 to Lesson 5. The lessons were very broad, but guided the design and implementation of all subsequent campaign cycles. The lessons are as follows:

1. Timing is important (section 7.6).
2. Advertising and attracting attention to the campaign must be an active, ongoing process (section 7.6).
3. In order to attract school participation and user attention to educate learners, a more engaging education approach was required (section 7.6).
4. Take into consideration the campaign’s implementation approach and its suitability for the targeted audience (section 7.6).
   a. Target a limited audience with a campaign suited to them (Section 7.6).
   b. Ensure that the implementation of the evaluation method is suited to or takes into consideration the skills (technical and non-technical) of the audience being examined (section 8.6).
5. Methods used to evaluate campaign effectiveness should be efficient and simple to implement (section 7.6).
Cycle 1 of the action research process focused on the design and implementation of cybersecurity and cybersafety education campaigns. The lessons learned from the cycle thus related to the pedagogical considerations of such a campaign, the need to attract and hold the interest of the target audience, and the appropriate use of campaign role-players and resources. Lesson 6 to Lesson 13 were learned in this cycle. The lessons are as follows:

6. Providing distinct educational and evaluation components in the campaign provides learners with more opportunities and experiences from which they can learn the campaign’s intended teachings (section 8.6).

7. Designing and implementing the campaign and its materials to be in keeping with pedagogical principles can positively affect ‘learners’ educational experience and improve the campaign’s probable effectiveness (section 8.6).

8. Personalising official communication and interaction with the schools and target audience has a relationship with increased interest and participation in the campaign effort (section 8.6).

9. Obtaining principal and teacher commitment to participation and subscription to the campaign and its messages contributes to the competition being implemented and supported at the school (section 8.6).

10. Brand symbols should be carefully designed and actively incorporated into the campaign to relate to the cybersecurity or cybersafety messages (section 8.6).
   a. Brand symbols for cybersecurity campaigns should take into consideration how relevant their design is to the target audience (section 9.6.2).
   b. The adoption of brand symbols by the target audience is affected by the consistency of their incorporation in learning experiences, as well by the frequency with which learners are exposed to these symbols (section 11.5.3).

11. The use of existing resources and experts should be encouraged where possible, as a cybersecurity campaign is a multidisciplinary endeavour (section 8.6).
   a. Making use of existing resources and experts increases a campaign’s adaptability (section 10.6).

12. Incentives to encourage participation should be well defined, and thoroughly explained at the start of the campaign and be fairly allocated (section 8.6).

13. Personalising and contextualising the campaign and its resources to suit the needs of the target audience can lead to an increased level of internalisation (section 8.6).
Cycle 2 of the action research process focused in greater depth on designing the campaign to be as scalable or transferable to as many contexts and target audiences as possible. However, a key factor was making effective use of resources without reducing the quality of the cybersecurity and cybersafety education experience for the target audience. Lesson 14 to Lesson 16 were learned in Cycle 2. These lessons are as follows:

14. Campaign role-players must be provided with appropriate and sufficient resources to fulfil their roles effectively (section 9.6.1).

15. Content creation should take into consideration that the availability of resources, the degree of required contextualisation and degree to which a campaign is adaptable are symbiotic characteristics of campaign material (section 9.6.4).

16. Campaign resources and activities placing strong emphasis on particular content support and encourage content adoption and internalisation. But exposure to the materials and activities cannot guarantee content internalisation if the learner is opposed to the content's message (section 9.6.5).
   a. Target audiences are more likely to accept cybersecurity lessons that reflect their own pre-existing beliefs about the issue or related issues (section 10.5.3.2).

Cycle 3 confirmed many of the action research process focussed adding formalised education components to the campaign. These formalised components were to enable the teachers (education experts) to participate and contribute in their school's cybersecurity education experience. Lesson 17 was learned as a result of Cycle 3. This lesson is as follows:

17. A cybersecurity education campaign should enable the continuous education or multiple opportunities for education of the target audience by providing several levels of education and the relevant resources (scaffolding) (section 10.6).
   a. Providing learners with multiple learning opportunities, of consistent quality, enables them to review and reflect upon material and thus encourages them to internalise the taught concepts (section 11.5.3).

Cycle 4 for of the action research process focussed on determining whether what was being achieved by the campaign was the intended result. This was done by examining whether the message being interpreted by the target audience aligned with the message the educational campaign intended to communicate. Lesson 18 was learned as a result of Cycle 4. This lesson is as follows:
18. Measures must be put in place to enable the evaluation of the campaign’s effectiveness of communicating with the target audience and thereby meeting its educational objectives (section 11.6.2).

Lessons were verified and expanded on in various cycles of the action research. This section briefly discussed the lessons from the perspective of the broad cycles in which they were originally identified. This concludes the summary of the lessons learned during the action research process.

12.3 Summary of results

The primary objective of the study, as presented in section 1.7, was to demonstrate how existing theory could be modified for use in addressing the human factor in information security. In order to achieve this objective, several sub-objectives were achieved.

The first sub-objective was to “determine the factors that should be considered in the design and implementation of information security and cybersecurity and cybersafety education campaigns”. Chapter 3 examined existing literature in the field of information security and cybersecurity and cybersafety education. The chapter reviewed numerous sources. The reviews considered the broad thematic questions of: who had been or should be educated about cybersecurity and safety; what they had have been or should be educated about; and how they were educated. The last question included the consideration of specific underlying components, issues and processes of the educational effort highlighted in the study as being important, e.g. pedagogical design, delivery or presentation recommendation and methods. Lessons learned from the literature were incorporated into the design of the initial intervention in the study’s action research process. This achieved the first sub-objective and thus answered the first research question stated in section 1.6, namely “What factors should be considered in the design and implementation of information security and cybersecurity and cybersafety education campaigns?”.

The second sub-objective was to “identify existing theories from the fields of education and communication studies that can play a role in the improvement of the design and implementation of cybersecurity and cybersafety education campaigns”. Chapter 5 addressed this objective.

A variety of theories from the fields of education and communication studies could be applied to a cybersecurity and cybersafety education campaign. Investigating all of them was beyond the scope of the study, however. Chapter 5 introduced the pedagogy of brain-compatible education,
and a media and communication theory, active audience theory as appropriate theories for application to cybersecurity and cybersafety education campaigns.

Chapter 6 included explanations about how brain-compatible education principles were applied to the design and implementation each year of the cybersecurity and cybersafety education campaign. The suitability of applying brain-compatible education principles to information security and cybersecurity education materials was investigated, peer-reviewed and published (Reid and Van Niekerk 2013b). Feedback was received from the reviewers and conference attendants. The feedback was taken into consideration and applied to a further cybersecurity education effort and peer-reviewed and published in a journal (Reid, R., & Van Niekerk, J. 2014).

The fourth cycle (Cycle 4, 2015) presented in Chapter 11 demonstrated how active audience theory, specifically Stuart Hall’s Encoding/decoding model could be used to determine whether the school learner target audience had interpreted the campaign message(s) as these were intended to be interpreted. Results from the application of this theory were initially peer-reviewed and published (Reid and Van Niekerk, 2015). Feedback was received from expert researchers in the fields of information security and cybersecurity. This was used to refine the application of the theory. The results of this refined application were peer-reviewed and published in a journal (Reid and Van Niekerk, 2016).

In all, this answered the second research question of the study, namely “What existing theories from the fields of education and communication studies can play a role in the improvement of the design and implementation of cybersecurity and cybersafety education campaigns?”

The third sub-objective was to “investigate, through an action research process, the effect of a variety of cybersecurity and cybersafety educational interventions for school children”. This sub-objective was met in Chapter 6 to Chapter 11. The chapters presented a report on the action research process undertaken to design, implement and refine a cybersecurity and cybersafety education campaign targeted at school children. The chapter outlined the design and implementation changes and the results of the interventions. This included the impact of the campaign on the targeted learners’ knowledge of cybersecurity and cybersafety. While meeting this third sub-objective through various iterations of the action research process, many lessons were learned about factors to consider in the design and implementation of cybersecurity and cybersafety education campaigns targeting the youth. These lessons were discussed in each research cycle, section 12.2 and can be seen in Table 12.1 alongside the section number they were first outlined in.
Findings derived from research conducted to meet the third objective resulted in several publications. Two categories of publication exist in relation to the third sub-objective: firstly, those relating to the effect of the various cybersecurity and cybersafety educational interventions on their targeted learners; and secondly, those relating to the use of a pedagogically designed educational game that teaches simple cybersecurity and cybersafety lessons to young children.

The findings from various interventions made throughout the cycles were peer-reviewed, published, and refined. In chronological order, the results were published as Van Niekerk, Thomson and Reid (2013), Reid and Van Niekerk (2014b) and finally Reid and Van Niekerk (2015). In the case of the latter two publications, feedback received during the peer-review and publication of each preceding publication was used to refine the research and its implementation.

During the action research process, a brain-compatible version of the board game “Snakes and Ladders” was developed to teach children cybersecurity and cybersafety lessons. This game is described in detail in section 8.3.2.1.2. The game was used in Cycle 1 to Cycle 4 of the campaign reported on in Chapter 8 to Chapter 11. The results of the first evaluation of the game’s use and its effect as a pedagogically designed educational game on the cybersecurity and cybersafety awareness of school learners were initially presented at the Kaspersky “Cybersecurity for the Next Generation” Student Conference: Asia-Pacific & MEA (2013) in Singapore. This conference was an international competition. The paper was presented in the final round of the competition at the 2013 Kaspersky “Cybersecurity for the Next Generation” Student Conference in London. Feedback on the presentation was sought from participants and cybersecurity experts. Feedback was also received at both the regional and final rounds of the competition. This feedback indicated that the experts considered the results of the case study to be promising and believed that the game had potential for use in educating children about cybersecurity. However, the experts did recommend that further studies be conducted using different participants. These additional studies were conducted and published as Reid and Van Niekerk (2014).

This answered the third research question of the study, namely “What effect do various cybersecurity and cybersafety educational interventions have on school children’s cybersecurity and cybersafety knowledge?”

In meeting the three sub-objectives of the study, the primary objective, “produce actionable knowledge, which offers guidance for designing and implementing education campaigns that educate school learners about cybersecurity”, was achieved. This answered the primary research
question of this thesis, namely, “What factors should be considered when designing and implementing education campaigns to educate school learners about cybersecurity?”

12.4 Summary of contributions

The work reported on in this thesis led to four primary contributions to the body of knowledge in the field of cybersecurity and cybersafety education. A brief summary of these contributions follows below:

- The first contribution of this study was in providing insight into an education campaign designed to contribute to the fostering of a culture of cybersecurity and cybersafety among school children. Through the implementation of an action research process implemented in 2011 (pilot) an understanding was formed about the effect of various cybersecurity and cybersafety educational interventions targeting school children. The effect on learners’ cybersecurity and cybersafety awareness was measured repeatedly. The main contribution was the lessons learned and confirmed in the iterative campaign cycles. These lessons can offer guidance in the design and implementation of education campaigns about cybersecurity and cybersafety designed for school learners. The lessons are presented as actionable knowledge in Table 12.1.

- The second contribution of this study was to show how brain-compatible principles could be applied in a pedagogical design and how an educational game could teach young children about basic cybersecurity and cybersafety practices. Education through gameplay is a novel approach to educating the youth about cybersecurity and cybersafety. Educational experiences should, however, be guided by pedagogy. The purpose of brain-compatible principles is to manipulate a learning environment directly so as to foster learners’ cognitive growth and understanding. When applied to educational material, the principles guide educators in the definition and selection of appropriate educational activities and presentation techniques. Brain-compatible education is suitable for most learners. The application of brain-compatible education principles to the design and development of games is not unique per se; however, as far as could be determined, the application of the principle to the design and development of cybersecurity education games and experiences had never been reported on outside of this study.

- The third contribution of this study was to show how active audience theory could be used in the evaluation of learners’ interpretation and internalisation of the campaigns taught
cybersecurity and cybersafety concepts. In the fourth cycle (2015) of the action research process reported upon here, an issue of interest that arose was the need to determine whether the audience had interpreted the campaign message(s) in the way that had been intended. This study has made a unique contribution by demonstrating how active audience theory, specifically Stuart Hall’s Encoding/decoding mode, can be adapted and used to analyse whether a learner’s interpretation of the cybersecurity campaign’s message corresponds to the interpretation the campaign was designed to convey to the target audience.

- The fourth contribution of this study was to provide some details about how a culture of cybersecurity and cybersafety would change as it moved away from an organisational context. This was an influential theme in this study. As part of this research, the possible role of general living systems theory in understanding the complex nature of cybersecurity was explored, peer-reviewed and published as Reid, Van Niekerk and Renaud (2014). However, as there is a well-established tradition of viewing information security culture using Schein’s model of corporate culture, this exploration was abandoned. Future research could continue to explore this complex and multi-layered view of cybersecurity. A second view of how a culture of cybersecurity could be differentiated from information security was simultaneously explored. This second view was also peer-reviewed and published as Reid and Van Niekerk (2014).
### Table 12:1 Actionable knowledge reference table

<table>
<thead>
<tr>
<th>Actionable Knowledge</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1  Timing is important.</td>
<td>7.6</td>
</tr>
<tr>
<td>L2  Advertising and attracting attention to the campaign must be an active, ongoing process.</td>
<td>7.6</td>
</tr>
<tr>
<td>L3  In order to attract school participation and user attention to educate learners, a more engaging education approach was required.</td>
<td>7.6</td>
</tr>
<tr>
<td>L4  Take into consideration the campaign’s implementation approach and its suitability for the targeted audience.</td>
<td>7.6</td>
</tr>
<tr>
<td>L4A Target a limited audience with a campaign suited to them.</td>
<td>7.6</td>
</tr>
<tr>
<td>L4B Ensure that the implementation of the evaluation method is suited to or takes into consideration the skills (technical and non-technical) of the audience being examined.</td>
<td>8.6</td>
</tr>
<tr>
<td>L5  Methods used to evaluate campaign effectiveness should be efficient and simple to implement.</td>
<td>7.6</td>
</tr>
<tr>
<td>L6  Providing distinct educational and evaluation components in the campaign provides learners with more opportunities and experiences from which they can learn the campaign’s intended teachings.</td>
<td>8.6</td>
</tr>
<tr>
<td>L7  Designing and implementing the campaign and its materials to be in keeping with pedagogical principles can positively affect ‘learners’ educational experience and improve the campaign’s probable effectiveness.</td>
<td>8.6</td>
</tr>
<tr>
<td>L8  Personalising official communication and interaction with the schools and target audience has a relationship with increased interest and participation in the campaign effort.</td>
<td>8.6</td>
</tr>
<tr>
<td>L9  Obtaining principal and teacher commitment to participation and subscription to the campaign and its messages contributes to the competition being implemented and supported at the school.</td>
<td>8.6</td>
</tr>
<tr>
<td>L10 Brand symbols should be carefully designed and actively incorporated into the campaign to relate to the cybersecurity or cybersafety messages.</td>
<td>8.6</td>
</tr>
<tr>
<td>L10A Brand symbols for cybersecurity campaigns should take into consideration how relevant their design is to the target audience.</td>
<td>9.6.2</td>
</tr>
</tbody>
</table>

Continued on next page.
<table>
<thead>
<tr>
<th>Actionable Knowledge</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>L10B The adoption of brand symbols by the target audience is affected by the</td>
<td>11.5.3</td>
</tr>
<tr>
<td>consistency of their incorporation in learning experiences, as well by the</td>
<td></td>
</tr>
<tr>
<td>frequency with which learners are exposed to these symbols.</td>
<td></td>
</tr>
<tr>
<td>L11 The use of existing resources and experts should be encouraged where possible,</td>
<td>8.6</td>
</tr>
<tr>
<td>as a cybersecurity campaign is a multidisciplinary endeavour.</td>
<td></td>
</tr>
<tr>
<td>L11A Making use of existing resources and experts increases a campaign’s</td>
<td>10.6</td>
</tr>
<tr>
<td>adaptability.</td>
<td></td>
</tr>
<tr>
<td>L12 Incentives to encourage participation should be well defined, and thoroughly</td>
<td>8.6</td>
</tr>
<tr>
<td>explained at the start of the campaign and be fairly allocated.</td>
<td></td>
</tr>
<tr>
<td>L13 Personalising and contextualising the campaign and its resources to suit the</td>
<td>8.6</td>
</tr>
<tr>
<td>needs of the target audience can lead to an increased level of internalisation.</td>
<td></td>
</tr>
<tr>
<td>L14 Campaign role-players must be provided with appropriate and sufficient</td>
<td>9.6.1</td>
</tr>
<tr>
<td>resources to fulfil their roles effectively.</td>
<td></td>
</tr>
<tr>
<td>L15 Content creation should take into consideration that the availability of</td>
<td>9.6.4</td>
</tr>
<tr>
<td>resources, the degree of required contextualisation and degree to which a</td>
<td></td>
</tr>
<tr>
<td>campaign is adaptable are symbiotic characteristics of campaign material.</td>
<td></td>
</tr>
<tr>
<td>L16 Campaign resources and activities placing strong emphasis on particular</td>
<td>9.6.5</td>
</tr>
<tr>
<td>content support and encourage content adoption and internalisation. But exposure to</td>
<td></td>
</tr>
<tr>
<td>the materials and activities cannot guarantee content internalisation if the learner</td>
<td></td>
</tr>
<tr>
<td>is opposed to the content’s message.</td>
<td></td>
</tr>
<tr>
<td>L16A Target audiences are more likely to accept cybersecurity lessons that reflect</td>
<td>10.5.3.2</td>
</tr>
<tr>
<td>their own pre-existing beliefs about the issue or related issues.</td>
<td></td>
</tr>
<tr>
<td>L17 A cybersecurity education campaign should enable the continuous education or</td>
<td>10.6</td>
</tr>
<tr>
<td>multiple opportunities for education of the target audience by providing several</td>
<td></td>
</tr>
<tr>
<td>levels of education and the relevant resources (scaffolding).</td>
<td></td>
</tr>
<tr>
<td>L17A Providing learners with multiple learning opportunities, of consistent quality,</td>
<td>11.5.3</td>
</tr>
<tr>
<td>enables them to review and reflect upon material and thus encourages them to</td>
<td></td>
</tr>
<tr>
<td>internalise the taught concepts.</td>
<td></td>
</tr>
<tr>
<td>L18 Measures must be put in place to enable the evaluation of the campaign’s</td>
<td>11.6.2</td>
</tr>
<tr>
<td>effectiveness of communicating with the target audience and thereby meeting its</td>
<td></td>
</tr>
<tr>
<td>educational objectives.</td>
<td></td>
</tr>
</tbody>
</table>
12.5 Publications stemming from the research

Publications stemming from this research study are listed in this section. This section presents only works that are relevant to this study and published during the research period.

12.5.1 Journal Publications


12.5.2 Conference Publications


### 12.6 Limitations of this research

Cybersecurity and cybersafety education is essential for all members of society who interact in cyberspace. However, there are no widely accepted guidelines for the design or implementation of cybersecurity and cybersafety education campaigns that aim to educate all groups. Educating all users was also beyond the scope of the study. Nevertheless, the study did provide insight into the implementation of a cybersecurity and cybersafety education campaign targeting school children. Lessons learned from these insights may be applicable to the design and implementation of a campaign for school learners.

### 12.7 Suggestions for further research

Currently, the lessons learned from this action research study on cybersecurity and cybersafety campaigns is applicable only to education campaigns targeting school learners. There is a need for guidelines of the design and implementation of cybersecurity and cybersafety education campaigns that target all cyberspace users in a society. Future research could examine how the lessons learned and the actionable knowledge could be adapted and applied to the design and development of cybersecurity and cybersafety campaigns targeting other audiences in different contexts. The use of pedagogically designed games that teach children cybersecurity and cybersafety lessons is also an interesting research area that should be explored in more depth.
References


Bruer, J. T. (2006). In Search of Brain-Based Education.


Alexandria, VA: Association for Supervision and Curriculum Development. 


References

*Meaning and perspective in the research process.* London: SAGE Publications.


October(10), 15–16.


Reid, R., & Van Niekerk, J. (2013b). Towards a Brain-Compatible Approach for Web-Based, Information Security Education. In S. Furnell, N. Clarke, & V. Katos (Eds.), European


References

http://www.cyberaware.org.za/


Smilkstein, R. (2011). *We’re born to learn: Using the brain’s natural learning process to create*
References


Appendix List

The following appendices are available on the included CD:

- Appendix A: Journal Publications stemming from this thesis
- Appendix B: Conference publications stemming from this thesis
- Appendix C: The human brain and learning
- Appendix D: Chapter 6 Figures and Tables
- Appendix E: Snakes and Ladders Instruments
- Appendix F: Cybersecurity and Cybersafety Curriculum
Appendix A: Journal Publications stemming from this thesis
Brain-compatible, web-based information security education: a statistical study

Rayne Reid and Johan van Niekerk

Institute of ICT Advancement, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

Abstract

Purpose – This paper aims to demonstrate that learners prefer brain-compatible cyber security educational material, over traditional presentation methods.

Design/methodology/approach – A prototype brain-compatible cyber security educational system was evaluated using a survey as a research instrument.

Findings – Presenting cyber security material in a brain-compatible manner is an effective way in which to stimulate the learners’ interest, engages them in the learning experience and motivates them to learn.

Originality/value – As far as could be determined, no previous studies showed the relevance of brain-compatible pedagogical techniques to cyber security education.

Keywords E-learning, Experiment, Brain-compatible education, Information security education, Empirical data

Paper type Research paper

1. Introduction

Information security education is one of the most fundamental components of any information security solution. It is this educational component of the security solution which is most prominently used to influence one of the security solutions greatest assets and threats, the human factor.

The “human factor” constitutes the weakest link in information security (Ahlfeldt et al., 2007). Users are often the cause of many security threats, and their actions account for a greater proportion of computer-related information loss than any other source of threat and are often more harmful than external threats (Chen et al., 2008; “NIST800-12,” 2004). This is because users problematically often lack the knowledge of those skills which are necessary for them to enable them to carry out their cyber security responsibilities and roles.

If this problem is to be combated, it is essential that the following two characteristics, which help to render a human being effective in his/her cyber security role are addressed, namely, knowledge about cyber security and the intent to behave in accordance with this knowledge (Van Niekerk, 2010).

To gain the required knowledge, users need to become aware of, and a subscriber to, information security practices. To achieve this, users of information resources must be

The financial assistance by the Vodacom/NMMU scholarship towards this research is also hereby acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not necessarily to be attributed to the sponsors.
educated about information security. However, not all courses would be suitable for providing this education effectively. This could be because of a number of factors, one of the more prominent being a possible lack of pedagogical theory in the course’s design. Puhakainen (2006) found that most current approaches towards information security education fail to pay sufficient attention to pedagogical theory. Therefore, it was recommended that a pedagogically sound course would be more effective at educating a learner.

Previous work presented how the presentation component of an information security educational course could be designed to adhere to a brain-compatible pedagogy (Reid et al., 2011). However, whether learners perceived this brain-compatible educational (BCE) format for cyber security educational material to be more appealing than the original material had not been experimentally verified. Therefore, using the past research’s prototype, this paper presents an experiment which tests whether learners perceived the BCE material as being more motivational, engaging and/or effective at meeting their educational needs than other approaches.

2. Methodology
The paper presents an experiment to verify the learners perceptions of the efficiency of a brain-compatible information security educational course compared to a non-brain-compatible information security educational course. The implementation of the experiment is explained in Section 3.1.4.

3. Experiment
An experiment was performed to determine whether web-based cyber security educational content that is presented in a brain-compatible manner is preferred by learners over the same content presented in a non-brain-compatible way. This section will present the research design of this experiment, as well as its results and analysis.

3.1 Research design
The research design involved the selection of an appropriate sampling method, and the development of the needed prototypes, research instruments and procedures.

3.1.1 Context. SEAT is a security education and training course at the Nelson Mandela Metropolitan University (NMMU), which targets students and the general public. Its objectives are: to improve awareness of the need to protect system resources and end-users; to develop the skills and knowledge of computer users, so they may securely perform their computer activities; to allow online access to a rich-source of security-related best practices; and to help end-users understand why security is part of their responsibilities, and how they impact their organizational employers security.

As a result of the choice of course and the research focus, other contextual parameters (target audience, course content and learning management system) were affected.

Because the demography of the target audience was not a primary research focus, a readily available target audience was selected. The target audience comprised fourth-year information security students at NMMU. With permission from the subject lecturer, these students were asked to participate in the experiment voluntarily. Eighty-three students consented to anonymously participate in the study.

The focus of the research was the effect of brain-compatible presentation of the material affected the learner’s perceptions of the material. Therefore, to ensure the integrity of the study, no characteristic besides the presentation could be changed. Therefore, the course material content included in the prototype implementation of the experiment comprised the same factual content which is included in an existing course.
The presentation of the material was redesigned to comply with the brain-compatible educational principles.

3.1.1 Brain-compatible education. Brain-compatible education involves teaching through the designing and orchestrating life-like, enriching and appropriate experiences for learners (Caine and Caine, 1991). It is a pedagogy which addresses multiple modes of learning, acknowledge outlets for creative presentation of learning, provide enough contrast to preclude boredom and contribute to a motivating context (Rogers and Renard, 1999). It accomplishes this by using effective teaching methods, techniques and approaches from all educational disciplines to enhance subject matter to be as appealing and learnable as possible for target students (Jensen, 2008). Its implementation is achieved through application of BCE principles (Table I).

Previous work showed that BCE principles can be applied in the Moodle 2.0 environment when developing an information security course, which is intended to be appealing and effective for a learner’s information security education experience (Reid and Van Niekerk, 2013). The original and redeveloped courses were used as prototypes within the experiment.

3.1.2 Prototypes. A prototype is an early sample built to test either a concept or a process or to act as something to be either replicated or learnt from. The purpose of the prototype is, therefore, to act as a test subject. For the purpose of this experiment, two prototypes were required:

(1) **Prototype A** – The original, unchanged SEAT material (SEAT) was required as a control “test” or placebo in the experiment. The original SEAT consisted of nine modules. Each module consisted of a single flash lesson and a related multiple choice quiz. The lessons content presentation consisted of text and related clipart images. An evaluation of the original SEAT showed that it lacked usability, which necessitated the redevelopment of the course.

(2) **Prototype B** – The modified material which was presented in a brain-compatible format (BCE-SEAT). The existing SEAT courses material to comply was redesigned for its presentation to comply with BCE principles. Suggested changes which were previously theorized possible by Reid et al. (2011) were included and expanded upon. The goal of such redevelopment was to make the material more appealing to the learner.

<table>
<thead>
<tr>
<th>Principle number</th>
<th>Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A learning experience should be as multi-faceted as possible; catering for many learning styles and providing as many opportunities for each learner to develop as possible</td>
</tr>
<tr>
<td>2</td>
<td>Positive emotions should be used to aid recognition and recall</td>
</tr>
<tr>
<td>3</td>
<td>It is necessary to repetitively review material to solidify recall and recognition</td>
</tr>
<tr>
<td>4</td>
<td>Both focused and peripheral attention of a learner should be involved in the learning process</td>
</tr>
<tr>
<td>5</td>
<td>Every brain simultaneously perceives and creates parts and wholes during the learning process</td>
</tr>
<tr>
<td>6</td>
<td>Relate all new material back to old material, thereby building new knowledge on old knowledge</td>
</tr>
<tr>
<td>7</td>
<td>Allow learners to progress through the course at their own pace</td>
</tr>
</tbody>
</table>

**Table I.** Brain-compatible education principles
Both prototypes are accessible as an e-learning course via Moodle. The experiment conducted in the experiment will compare the effectiveness of the new cyber security course material’s presentation against the older courses’ presentation. This will be done by measuring the learners’ perceptions of presentation of Prototype A as opposed to Prototype B. The learner’s perceptions were determined through the use of a research instrument.

### 3.1.3 Instrument
For the purposes of this study, the instrument is a questionnaire which was filled out anonymously and electronically by the experiment’s participants.

A questionnaire which was presented in the education-related research conducted by Du Plessis (2010) had measured factors such as motivation, engagement and other learner perceptions’ of course material. As its objective matched that of this research, and it was a verified instrument, this questionnaire was adapted to suit the parameters of this experiment. Modifications made the questions more specific to these experiments prototypes.

The modified questionnaire consisted of 41 questions which attempted to gauge the learners’ perceptions. Thirty-eight of the questions are close-ended while three are open-ended. The close-ended questions consist of multiple choices, yes/no and Likert scale questions, while the open-ended questions are opinion-based questions. Each of the closed-ended questions fell into one or more thematic category of possible learner perceptions. These results of the thematic categories were what would be used during the analysis. The Themes of analysis and classification of the questions relevant to each theme are shown in Table II.

<table>
<thead>
<tr>
<th>Theme number</th>
<th>Theme</th>
<th>Relevant questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Learner perception of whether the e-learning lesson material is presented in a more appealing way than the material to which they are exposed in real-world classrooms</td>
<td>1, 3, 16, 32, 33, 34</td>
</tr>
<tr>
<td>2</td>
<td>Learner perception of whether this type of e-learning course presentation format is enjoyable enough to want to use it in other subjects</td>
<td>2, 3, 17, 20, 22, 37, 32, 34, 35, 36</td>
</tr>
<tr>
<td>3</td>
<td>Learner perception of whether the learning experience is positive and enjoyable as a result of the e-learning delivery and presentation platform</td>
<td>2, 3, 20, 37, 38, 18, 19, 27, 30, 31</td>
</tr>
<tr>
<td>4</td>
<td>Learner perception of the increase in their knowledge as a result of the perceived effectiveness of the course</td>
<td>21, 38, 24, 25, 26, 35</td>
</tr>
<tr>
<td>5</td>
<td>Learner perception of whether the material’s presentation enhanced focus and heightened interest engagement</td>
<td>38, 6, 9, 18, 27, 29, 35</td>
</tr>
<tr>
<td>6</td>
<td>Learner perceptions and experiences of the motivational and emotional benefits derived from the presentation of the material</td>
<td>38, 7, 10, 30, 31, 35</td>
</tr>
<tr>
<td>7</td>
<td>Learner perception and opinions of the media-richness of the material’s presentation</td>
<td>12, 13, 18, 12, 14, 15, 25, 26</td>
</tr>
<tr>
<td>8</td>
<td>Learner perception of whether the presentation of the material promoted understanding of content</td>
<td>7, 13, 14, 15, 25, 26, 8, 13, 14, 23, 26, 28</td>
</tr>
<tr>
<td>9</td>
<td>Learner perception of whether the presentation of the material made the content more relatable</td>
<td>8, 13, 14, 23, 26, 28, 20, 38</td>
</tr>
<tr>
<td>10</td>
<td>Learner perception of whether the presentation of the material catered appropriately for the learners’ preferred learning styles and study habits</td>
<td>5, 11, 13, 18, 35</td>
</tr>
</tbody>
</table>

Table II. Themes of analysis in the research instrument
3.1.4 Implementation. The aim of this experiment is to determine whether the brain-compatible presentation design of SEAT, a cyber-security course, is perceived by learners as being more effective and suitable for their needs compared to other approaches. Therefore, a controlled comparison and analysis of the learners’ perceptions in relation to both the exploratory prototype and a control prototype is needed.

For the experiment, the 83 students who consented to anonymously participate in the study were randomly divided into two sample groups. The participants in both groups were sent a link to a Cyber Security course via e-mail.

The first group was sent the link and login details for the new SEAT material, which was presented in a brain-compatible format (Prototype-B). This group of learners will be referred to as Sample-A. The second group of learners was sent the link and login details for the original SEAT material (Prototype-A). This group was to act as the control group for the experiment and will, henceforth, be referred to as Sample-B. The e-mails also contained the instructions detailing how to progress through the course. They would be required to individually complete the material and questionnaire; at their own pace and convenience; within a two week period. Both groups were required to answer the same questionnaire (instrument) at the end of the course in question.

After the two week period had expired, only 69 of the original 83 learners had completed both the material and questionnaire. Of these participants, 35 students were Sample-A participants, while the remaining 34 students were Sample-B participants. However, the sample was deemed to be a sufficiently large sample to provide statistically meaningful data. Only the results gathered from the completed questionnaires will be discussed and analyzed in the next section.

3.2 Research results and analysis
This section will present the statistical interpretation of the results gathered via the questionnaire. Following this, it will then also provide the thematic analysis and interpretation of the results.

3.2.1 Statistical interpretation of results. All of the responses to the questionnaires were analyzed for statistical significance by the unit of statistical support at the NMMU. The survey comprised two main forms of questions, namely, yes/no questions and Likert scale questions. The yes/no questions were interpreted with the aid of a chi-square statistic, while the Likert scale questions were interpreted by means of a t-test.

For the chi-square statistic, a critical value of 6.625 was used to test the significance of the results with 99 per cent certainty ($\alpha = 0.01$). For a 95 per cent ($\alpha = 0.05$) certainty, the critical level would be 3.841. The questions with 95 per cent significance were not used in the formal evaluation of the value of the programme. However, it must be noted that several results which were not significant at 99 per cent approached the critical value for significance at the 95 per cent certainty level. Thus, if the $\chi^2_{0.99}$ is greater than 6.625 it would mean that the results are significant and that we are 99 per cent certain of this significance. If $\chi^2_{0.95}$ is greater than 3.841 the results could also be deemed significant but only at a 95 per cent level of certainty of the result. In the case of this study the 99 per cent level of significance has been used. However, in some cases, the 95 per cent level of significance was considered in the analysis of results as a supporting statistic for Cramer’s V-value.

Cramer’s V-value is used to indicate practical significance. The results of the Cramer’s V-value were interpreted as a value less than 0.1 being of small practical significance, a
V-value of less than 0.3 and greater than 0.1 being of medium significance and a V-value of 0.5 or greater being of large practical significance. In the case of the thematic statistical analysis, a $t$-test was used. Like the chi-square statistics, the $p$-value was what indicated statistical significance. Its interpretation was also the same. For all the significant $t$-test values, the Cohen’s $d$-value indicates the degree of practical significance.

3.2.2 Analysis and interpretation. This section will present the thematic analysis based on a statistical analysis which was performed according to the question grouping in Table II. The findings to be presented in this section will be identified as being either statistically significant or not.

The analysis of the themes will be conducted systematically. The themes will be referred to according to the numbering system used in Table II. The thematic analysis will, first, analyse the themes in terms of the Likert scale question findings. The results based on the overall statistical findings will then be discussed and analysed (Table III).

Theme 1. For Theme 1, the analysis of the data results gathered via the Likert scale indicate that, thematically, there was a 99 per cent statistically significant certainty that the learners found the B material to more appealingly presented than the material to which they were exposed in the real-world. This indicates a strong affirmation of the theme.

For the yes/no questions, questions 1 and 16 results both have medium practical significance but differ between the 95 per cent and 99 per cent certainty levels. These results indicate a definite that the learners had perceived the material to be appealing. In comparison, Question 3 (relating to learners’ enjoyment of the material) had a small practical significance and no statistical degree of certainty. This insignificant result suggests that, although the learners had found the material appealing, they had not necessarily enjoyed it. Overall, however, the yes/no question category for this theme may interpret as moderate confirmation of theme 1.

Ultimately, the findings of this theme conclusively indicate that those learners who were exposed to the brain-compatible material had positively perceived the materials to be more appealingly presented than the material to which they were exposed in real-world classrooms (Table IV).

Theme 2. For Theme 2, the findings of the Likert scale questions indicate that there is a moderate practical significance and a 95 per cent level of statistically significant certainty that the learners preferred the SEAT material, its presentation and e-learning platform to real-world classrooms.

<table>
<thead>
<tr>
<th>Mean</th>
<th>Mean</th>
<th>$t$-value</th>
<th>$df$</th>
<th>$p$</th>
<th>Valid $N$</th>
<th>Valid $N$</th>
<th>$SD$</th>
<th>$SD$</th>
<th>Cohen’s $d$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.84</td>
<td>3.25</td>
<td>3.63</td>
<td>67</td>
<td>0.000554</td>
<td>35</td>
<td>34</td>
<td>0.54</td>
<td>0.78</td>
<td>0.87</td>
</tr>
</tbody>
</table>

Table III. Theme 1 $t$-tests

Large practical significance

<table>
<thead>
<tr>
<th>Mean</th>
<th>Mean</th>
<th>$t$-value</th>
<th>$df$</th>
<th>$p$</th>
<th>Valid $N$</th>
<th>Valid $N$</th>
<th>$SD$</th>
<th>$SD$</th>
<th>Cohen’s $d$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.07</td>
<td>3.74</td>
<td>2.35</td>
<td>67</td>
<td>0.021856402</td>
<td>35</td>
<td>34</td>
<td>0.56</td>
<td>0.63</td>
<td>0.57</td>
</tr>
</tbody>
</table>

Table IV. Theme 2 $t$-tests

Medium practical significance
The yes/no questions varied in practical. Questions 2, 3 and 20 indicated small practical significance, Question 32 indicated medium practical significance and Questions 17 and 22 indicated a large practical significance. Questions 2 and 3 had no percentile of certainty; Questions 20 and 37 had 95 per cent level of certainty of statistical significance, while questions 17 and 22 had 95 per cent level of certainty of statistical significance. Questions 2, 3, 20 and 37 dealt with enjoyment and all had either no or low practical and statistical significance. Comparatively, Questions 17 and 22 dealt with the learners’ perception of enjoying or liking the presentation of the materials enough to consider having their other subject materials similarly presented. They had a large practical significance and were statistically significant within the 99 per cent percentile.

The findings of the yes/no questions indicated low levels of statistical evidence that the learners who had been exposed to the brain-compatible material would enjoy material presented in this manner. However, in contrast to this, they showed significant interest in having future subjects material similarly presented.

Ultimately, the combined results of both categories indicate moderate confirmation that learners had positively perceive the e-learning, brain-compatible course presentation format as enjoyable and that they would be willing to learn using a similar approach in other subjects (Table V).

Theme 3. The analysis of the Likert scale questions data indicates that, thematically, the learners perceived the experience to be positive and enjoyable as a result of the e-learning delivery and presentation platform. These findings were of high to moderate statistical significance with 99 per cent certainty. It is of medium practical significance.

The questions in the yes/no category ranged in practical significance and certainty levels. Questions 2 and 3 had no degree of statistical certainty, question 20 had a 95 per cent level of certainty and questions 37 and 38 were statistically significant with a 99 per cent level of certainty. Question 37 was of medium practical significance, questions 2, 3 and 20 were of small practical significance and questions 37 and 38 were of large practical significance.

Questions 2, 3, 20 and 37 all dealt with the enjoyment of the material and its presentation. Question 38 explored the learners’ perceptions that the material had improved their learning experience by catering for their preferred learning styles. The findings of these questions indicate a small to moderate prospect of the learners having had a positive learning experience as a result of their enjoyment of the material. Additionally, the findings indicate that there is a large probability of learners having enjoyed the material as a result of both its presentation and the platform’s abilities to cater for their learning preferences.

Overall, this analysis concludes that there is a moderately good probability of the learners enjoying the material because they perceived it to cater to their preferred learning styles. However, because of the inherent “work” factors, there is a lower probability that the enjoyment is recreational (Table VI).

<table>
<thead>
<tr>
<th>Mean 1</th>
<th>Mean 2</th>
<th>t-value</th>
<th>df</th>
<th>p</th>
<th>Valid N</th>
<th>Valid N</th>
<th>SD</th>
<th>SD</th>
<th>Cohen’s d</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.23</td>
<td>3.79</td>
<td>0.21</td>
<td>67</td>
<td>0.00464323</td>
<td>35</td>
<td>34</td>
<td>0.55</td>
<td>0.63</td>
<td>0.71</td>
</tr>
</tbody>
</table>

Medium practical significance

Table V. Theme 3 t-tests
Theme 4. The analysis of the Likert scale questions data indicates that, thematically, there is a high statistical certainty that the learners perceived the experience to be both positive and enjoyable because of the e-learning delivery and presentation platform. These findings are statistically significant with 95 per cent certainty, but are not practically significant.

The questions within the yes/no category had mixed significance. Question 21 dealt with the perception of the knowledge, which had been acquired. The findings had small practical significance but no statistical level of certainty. In comparison, Question 38 had a large level of practical significance and a 99 per cent level of certainty. It dealt with the learners’ perceptions of the material promoting learning via a presentation which appealed to the learners’ learning style and media-richness preferences. Question 38 was of greater importance than question 21.

Overall, the learners’ perception of the knowledge gain as a result of the course effectiveness was moderately low. However, this was not the focus of the research and it is also likely that the material was too simplistic to gauge accurately whether the material had ensured learning (Table VII).

Theme 5. The analysis of the Likert scale questions data indicate that, thematically, there is high statistical significance and 99 per cent certainty that Sample-A perceived that the presentation of the material had promoted a level of heightened focus and attracted their interest. These results are of large practical significance. The yes/no question (Question 38) results concurred with the above result.

Ultimately, the findings of this thematic analysis category indicate that the learners had positively perceived that the presentation of the material had promoted a level of heightened focus and interest during the learning experience (Table VIII).

Theme 6. The analysis of the Likert scale questions data indicates that, thematically, there is a moderate 95 per cent statistical certainty that Sample-A. These findings were of medium practical significance. Question 38 (the yes/no question) concurred with this finding, but with greater (99 per cent) statistical significant certainty.

<p>| Table VI. | Theme 4 t-tests |</p>
<table>
<thead>
<tr>
<th>Mean</th>
<th>Mean</th>
<th>t-value</th>
<th>df</th>
<th>p</th>
<th>Valid N</th>
<th>Valid N</th>
<th>SD</th>
<th>SD</th>
<th>Cohen’s d</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>4.11</td>
<td>3.99</td>
<td>67</td>
<td>0.387569011</td>
<td>35</td>
<td>34</td>
<td>0.56</td>
<td>0.60</td>
</tr>
<tr>
<td>No practical significance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| Table VII. | Theme 5 t-tests |</p>
<table>
<thead>
<tr>
<th>Mean</th>
<th>Mean</th>
<th>t-value</th>
<th>df</th>
<th>p</th>
<th>Valid N</th>
<th>Valid N</th>
<th>SD</th>
<th>SD</th>
<th>Cohen’s d</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3.98</td>
<td>3.48</td>
<td>67</td>
<td>0.000065</td>
<td>35</td>
<td>34</td>
<td>0.46</td>
<td>0.52</td>
</tr>
<tr>
<td>Large practical significance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| Table VIII. | Theme 6 t-tests |</p>
<table>
<thead>
<tr>
<th>Mean</th>
<th>Mean</th>
<th>t-value</th>
<th>df</th>
<th>p</th>
<th>Valid N</th>
<th>Valid N</th>
<th>SD</th>
<th>SD</th>
<th>Cohen’s d</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>4.16</td>
<td>3.88</td>
<td>67</td>
<td>0.02671154</td>
<td>35</td>
<td>34</td>
<td>0.49</td>
<td>0.53</td>
</tr>
<tr>
<td>Medium practical significance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Overall, Theme 6 found that there is a moderately high probability of the learners perceiving the presentation of the brain-compatible cyber security material to be both motivational and beneficial (Table IX).

Theme 7. The analysis of the Likert scale questions data in the research instrument indicates that, thematically, there is a high to moderate statistical certainty that those learners, who had access to the brain-compatible material, positively perceived the presentation of the material to promote both studying and learning as a result of its media-richness. These results are statistically significant with 99 per cent certainty, and that they are of a medium practical significance.

Overall, this theme’s analysis indicates a moderately high probability that the future exposure of learners to the presentation of brain-compatible cyber security material would result in the learners perceiving the media richness of the material to be of benefit to their learning experiences (Table X).

Theme 8. The analysis of the Likert scale questions data indicates that, thematically, there is a high statistical certainty (99 per cent) that Sample-A, positively perceived the presentation of the material to have promoted their understanding of the content. This result is of large practical significance. Therefore, the findings of this thematic category indicate a high probability of those learners who have been exposed to the presentation of the brain-compatible material, perceiving the material to be highly conducive to their understanding of the concepts being taught (Table XI).

Theme 9. The analysis of Likert scale questions data indicates that, thematically, there is a moderate statistical certainty that those learners, who had access to the brain-compatible material, positively perceived that the presentation of the material had rendered the content more relatable. A t-test indicates that these results are statistically significant with 95 per cent certainty, and that they are of a medium practical significance.

<table>
<thead>
<tr>
<th>Mean</th>
<th>Mean</th>
<th>t-value</th>
<th>df</th>
<th>p</th>
<th>Valid N</th>
<th>Valid N</th>
<th>SD</th>
<th>SD</th>
<th>Cohen's d</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.00</td>
<td>3.57</td>
<td>2.73</td>
<td>67</td>
<td>0.008015619</td>
<td>35</td>
<td>34</td>
<td>0.62</td>
<td>0.69</td>
<td>0.66</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Medium practical significance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mean</th>
<th>Mean</th>
<th>t-value</th>
<th>df</th>
<th>p</th>
<th>Valid N</th>
<th>Valid N</th>
<th>SD</th>
<th>SD</th>
<th>Cohen's d</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.25</td>
<td>3.92</td>
<td>3.10</td>
<td>67</td>
<td>0.002860299</td>
<td>35</td>
<td>34</td>
<td>0.48</td>
<td>0.41</td>
<td>0.75</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Large practical significance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mean</th>
<th>Mean</th>
<th>t-value</th>
<th>df</th>
<th>p</th>
<th>Valid N</th>
<th>Valid N</th>
<th>SD</th>
<th>SD</th>
<th>Cohen's d</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.05</td>
<td>3.77</td>
<td>2.16</td>
<td>67</td>
<td>0.034338543</td>
<td>35</td>
<td>34</td>
<td>0.48</td>
<td>0.57</td>
<td>0.52</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Medium practical significance</td>
</tr>
</tbody>
</table>
Overall, the findings of this thematic category indicate that it is moderately probably that other learners who may be exposed to the presentation of the brain-compatible cyber security material would positively perceive that the presentation of the material had catered successfully for their preferred learning styles and study habits (Table XII).

Theme 10. The analysis of the Likert scale questions data indicates that, thematically, there is a moderate statistical certainty that Sample-A had positively perceived that the presentation of the material had catered for their preferred learning styles and study habits. These results are statistically significant with 95 per cent certainty and are of a medium practical significance.

The yes/no questions practical significance and certainty levels differed. Question 20 indicated that there was a small significance and a low certainty only relating to the learners’ probable enjoyment of the SEAT course format as a learning tool for the subject. Question 38 indicated a larger statistical and practical significance in that the learners had perceived the e-learning SEAT course material and presentation to more beneficial to them than other material, as it had catered for their preferred learning styles and media-richness requirements. Thematically, question 38 was of greater importance than question 20. Therefore, the yes/no question category will be interpreted as indicating a high probability those learners having positive perceptions within the theme.

Overall, it may be concluded that this theme has indicated a moderate probability of those learners, who are exposed to the presentation of the brain-compatible cyber security material, positively perceiving that the presentation of the material caters effectively for the learners’ preferred learning styles and study habits.

The majority of the thematic categorical analyses indicated that the brain-compatible material was beneficial to the learners’ cyber security educational experience. It may, thus, be concluded that presenting cyber security material in a brain-compatible manner is an effective way in which to stir the learners’ interest, engage them in the learning experience and motivate them to learn. Therefore, the learners had perceived this to be an effective cyber security educational approach.

4. Conclusions
This paper aimed to determine, via an experiment, whether a cyber-security course which is presented to be brain-compatible, was perceived by learners as being effective and suitable for their needs as compared to other approaches. The study and the analysis showed, from the perspective of the ten included themes, that learners had statistically significant perception of the new, brain-compatible presentation of the cyber security material to be more suitable and effective as regards their cyber security education needs.

<table>
<thead>
<tr>
<th>Mean</th>
<th>Mean</th>
<th>t-value</th>
<th>df</th>
<th>p</th>
<th>Valid N</th>
<th>Valid N</th>
<th>SD</th>
<th>SD</th>
<th>Cohen’s d</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.33</td>
<td>4.10</td>
<td>2.03</td>
<td>67</td>
<td>0.046190916</td>
<td>35</td>
<td>34</td>
<td>0.47</td>
<td>0.46</td>
<td>0.49</td>
</tr>
</tbody>
</table>

**Table XII.** Theme 10 t-tests

**Note:** The analysis of the Likert scale questions data indicates that, thematically, there is a moderate...
The authors have, therefore, empirically demonstrated that the material is effective and perceived as such by learners. Therefore, it will now be possible to use this material and its development as a foundation from which a development process may be derived for the design and development of the presentation tier of future cyber security education materials.

References


NIST800-12 (2004), Security, National Institute of Standards and Technology, Gaithersburg, MD.


Further reading

Corresponding author
Rayne Reid can be contacted at: s208045820@live.nmmu.ac.za

To purchase reprints of this article please e-mail: reprints@emeraldinsight.com
Or visit our web site for further details: www.emeraldinsight.com/reprints
Snakes and ladders for digital natives: information security education for the youth
Rayne Reid Johan Van Niekerk

Article information:
To cite this document:
Permanent link to this document:
http://dx.doi.org/10.1108/IMCS-09-2013-0063

Users who downloaded this article also downloaded:

Access to this document was granted through an Emerald subscription provided by emerald-srm:207521 []

For Authors
If you would like to write for this, or any other Emerald publication, then please use our Emerald for Authors service information about how to choose which publication to write for and submission guidelines are available for all. Please visit www.emeraldinsight.com/authors for more information.

About Emerald www.emeraldinsight.com
Emerald is a global publisher linking research and practice to the benefit of society. The company manages a portfolio of more than 290 journals and over 2,350 books and book series volumes, as well as providing an extensive range of online products and additional customer resources and services.
Emerald is both COUNTER 4 and TRANSFER compliant. The organization is a partner of the Committee on Publication Ethics (COPE) and also works with Portico and the LOCKSS initiative for digital archive preservation.

*Related content and download information correct at time of download.
Snakes and ladders for digital natives: information security education for the youth

Rayne Reid and Johan Van Niekerk

Institute of ICT Advancement, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

Abstract

Purpose – This paper aims to educate the youth about information security. Cyber technologies and services are increasingly becoming integrated into individual’s daily lives. As such, individuals are constantly being exposed to the benefits and risks of these technologies. Cyber security knowledge and skills are becoming fundamental life skills for today’s users. This is particularly true for the current generation of digital natives.

Design/methodology/approach – Within the design science paradigm, several case studies are used to evaluate the research artefact.

Findings – The authors believe that the presented artefact could effectively convey basic information security concepts to the youth.

Research limitations/implications – This study had a number of limitations. First, all the learner groups who participated in this study were too small to enable analysis of findings for statistical significance. Second, the data compiled on the long-term effectiveness of the game for Group B was incomplete. This limitation was the result of School B’s ethical concerns regarding learners being a vulnerable target audience.

Originality/value – This paper presents and evaluates a brain-compatible, information security educational game that can be used to introduce information security concepts to the youth from a very young age.

Keywords Case study, Information security, Brain-compatible education, Educational gameplay, Information security education

Paper type Research paper

1. Introduction

Information security knowledge and skills is becoming a crucial life skill for current information technology users. Users are becoming increasingly exposed to cyber security threats as their dependence on information technologies and services grows (Furnell et al., 2007).

This is occurring because information technologies and services are becoming increasingly integrated into our daily lives. Consequently, users have become over dependent on them. This is particularly true for the younger generations. The current

Professor R. Von Solms is acknowledged for his game content contribution. The financial assistance by the Vodacom/NMMU scholarship towards this research is also hereby acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not necessarily to be attributed to the sponsors.
digital natives (Generation Y, born in 1977-1994; and Generation Z, born in 1995-2012) account for > 23 million users of the Internet and other technologies (Schroer, 2012). Their communication, socialisation, creation and learning processes are all strongly affected by technology (Prensky, 2001). Therefore, these digital natives should be educated about information security.

However, how these users, particularly Generation Z, can be effectively educated about information security is problematic. Traditionally, learners look to their parents and teachers (customarily more knowledgeable individuals) to teach required knowledge and skills. However, in the case of information technology and security, the learners are often more technology-literate than their teachers. Additionally, “digital immigrant instructors, who speak an outdated language (that of the pre-digital age), are struggling to teach a population that speaks an entirely new language” (Prensky, 2001).

This paper introduces a novel approach for educating the youth about information security. It will present a brain-compatible, information security educational game.

2. Background
2.1 Information security education
Information security education provides the knowledge and skills needed to implement information security practices. Traditionally, information security has mainly been implemented in organisations. However, recent national legislation and cyber awareness campaigns (such as the campaigns run in the UK and USA) target the general public (UK Cabinet Office, 2011; White House, 2003). This target audience includes the youth whose educational needs differ from those of traditional organisational end-users.

2.1.1 Educational gameplay. This research is targeting the youth. The current generation often perceived learning as a “boring” activity because existing teaching methods are incompatible with how they learn (Tang and Hanneghan, 2011). Therefore, traditional approaches for information security education may not be suitable for this young target audience.

Educational studies have shown that school children have shown an interest in using the games for learning purposes (Roslina and Jaafar, 2009). This is an educational approach that will build on natural learning methods used by the young of each species to gather important life skills. Fun education is an effective mechanism for children, as it engages their interest and discourages them from disassociating from what is being learnt (Reid et al., 2011). Not all games are necessarily educational. Compliance with a proven pedagogy increases the games potential for being an effective education tool. This research complies with the brain-compatible pedagogy.

2.1.2 Brain-compatible education. Brain-compatible education (BCE) is a formal pedagogy encompassing educational principles, methods and techniques which endeavour to teach subject matter in a manner and format which is naturally complementary to the physical and psychological processing functions of the brain (Caine et al., 2005; Jensen, 2008).

Overall, the techniques aim at attracting the learner’s attention and ensuring that the learner processes the educational experience in a way that promotes the extraction of meaning from the material (Caine & Caine, 1991). During an educational experience, it achieves this by stimulating the sections of the brain that are involved in the learning practices. This encourages learners to process information more effectively so as to
To ensure maximum understanding, retention and recall of learnt material (Banikowski, 1999).

BCE includes several neurologically sound principles as a general theoretical foundation (Caine & Caine, 1991). Table I lists eight of these principles.

The purpose of brain-compatible principles is to manipulate a learning environment directly so as to foster learners cognitive growth and understanding (Lombardi, 2008). These principles have been effectively used in real-world classrooms and some online environments in the presentation of formal lessons. When applied to educational material, the principles guide educators in the definition and selection of appropriate educational activities and presentation techniques.

Some of these principles will be applied to the creation of the research artefact. The next section will present the methodology followed by this research.

### 3. Methodology

This research was conducted in compliance with the seven guidelines for conducting research within the design – science research paradigm, as described by Hevner et al. (2004). This section will detail how this research has complied with each guideline:

- **Design as an artefact**: This guideline recommends the production of a viable artefact. A tangible, brain-compatible, information security snake and ladder board game was designed and developed during the research process.

- **Problem relevance**: The objective of the research is to solve an important and relevant problem. Cyber security is a topic that is seldom addressed in current South African school environments. Until recently, this has been an acceptable practice. However, the current generation is growing up as digital natives who are constantly exposed to information technologies and related threats. Therefore, the digital generation (children) need to be educated about cyber security.

- **Design evaluations**: This guideline states that utility, quality and efficacy of a design artefact must be rigorously demonstrated. BCE is a formal pedagogy. The artefact developed by this research was developed in compliance with this

<table>
<thead>
<tr>
<th>No.</th>
<th>Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A learning experience should be as multifaceted as possible, catering to as many learning styles as possible and providing as many opportunities for each learner to develop as possible</td>
</tr>
<tr>
<td>2</td>
<td>Positive emotions should be used to aid recognition and recall</td>
</tr>
<tr>
<td>3</td>
<td>Relate all new material back to old material and, thereby, build new knowledge on old knowledge</td>
</tr>
<tr>
<td>4</td>
<td>The search for meaning is innate and occurs through patterning</td>
</tr>
<tr>
<td>5</td>
<td>Every brain simultaneously perceives and creates parts and wholes during the learning process</td>
</tr>
<tr>
<td>6</td>
<td>It is necessary to review material repetitively to solidify recall and recognition</td>
</tr>
<tr>
<td>7</td>
<td>Both the focused and peripheral attention of a learner should be involved in the learning process</td>
</tr>
<tr>
<td>8</td>
<td>Allow learners to progress through the course at their own pace</td>
</tr>
</tbody>
</table>

**Source:** Reid et al. (2011)
pedagogy’s principles. Additionally, the suitability and effectiveness of the artefact were evaluated by means of multiple case studies (further explanation in subsection 3.1).

• **Research contributions:** This guideline states that a problem must be solved by the research. The contributions which have been derived from this research are as follows:
  – the use of brain-compatible pedagogy in the development of an information security educational game (explanation in Section 3.2.1); and
  – the artefact itself, which is a tangible result of the research.

• **Research rigor:** The guideline recommended that rigorous methods be used in the creation and evaluation of the research artefact. This guideline was applied by:
  – complying with brain-compatible pedagogical principles in the artefact’s design; and
  – verifying the design and effectiveness via multiple case studies (see subsection 3.4).

• **Design as a search process:** This guideline requires that the creation of the artefact be designed using an iterative “searching” process. The board game’s design process adhered to this stipulation.

• **Communication of research:** The final guideline recommends that the research results be presented to affected audiences. This has been fulfilled through the:
  – distribution of the brain-compatible, information security games to primary schools;
  – publication of the pilot study’s results at the WISE conference (Reid and Van Niekerk, 2013); and
  – communication of further research conducted within this article.

This section demonstrated how this research complies with the design research paradigm. The next section will elaborate on the design of the artefact and its evaluation.

### 3.1 Case studies

This evaluation portion of the research will follow procedures from the case study protocols described by Yin (2009). The context of the case study was presented within the previous section as part of the problem relevance. The rest of this paper will present the research artefact; the research instrument and the implementation details of the case studies. Finally, the results and analysis of the research will be presented with accompanying conclusions which have been reached.

### 3.2 The artefact

The artefact is targeted at a primary school audience. Therefore, the following characteristics were considered while creating the artefact: age-appropriateness, content, user-friendliness, learnability and the potential for compliance with BCE principles.

Existing children’s games, which targeted this age group, were considered as the basis for the artefact’s design. “Snakes and Ladders”, a popular board game played by
children worldwide, was chosen as the artefact’s foundation. The reasons this game was chosen are as follows:

- having existed since the 2nd century in India, it is a popular game, rules of which are known to the target audience (Avedon, 2010);
- its original purpose of teaching children the difference between “good and evil” is similar to teaching children good and bad information security lessons (Avedon, 2010);
- third, it currently targets children aged ≥ 7 years; and
- pedagogical principles and appropriate information security educational content could be easily incorporated into the design.

The design, content and game play rules of the developed artefact will be discussed in the below subsections.

3.2.1 Design. This section will present the reasons why “Snakes and Ladders” was selected as a good redevelopment candidate for this research. These reasons will also be linked to implementation considerations from a BCE perspective. The focus of this section is, therefore, the presentation design.

First, the game had to cater for multiple learners’ learning rates. BCE advocates self-paced progression (Principle 8). The game achieved this via the turn-based play, which requires the player to throw dice and move a token, and read a lesson. This allowed the learners to play and learn at their own pace, while encouraging progression.

Second, the game’s design had to be interactive and “fun”. This was necessary to provide a social and communicative, peer-supported learning experience. This was considered essential, as it implements Principle 1 by appealing multiple learning styles, especially those favoured by kinaesthetic and auditory (social) learners. Additionally, these characteristics gain and hold the learner’s interest/focus, while positively stimulating their emotions (Principles 7 and 2).

The “fun factor” of the game is especially aimed at appealing to the learner’s positive emotions (Principle 2). This allows a learner to focus, learn and retain learned content better. Aspects of the game’s design appealing to this principle include: a game’s inherent fun, interactive and socially competitive nature; and its reinforcement mechanisms which encourage changes in emotional state (e.g. happiness for ascending a ladder). The incentive of winning also increases the fun factor and appeals to Principle 2 while encouraging progression through the game (Principle 8).

The colours used on the board also aimed to influence the state of the learner’s emotions and focus, thereby implementing Principles 2 and 7. The background of the board’s squares were coloured various shades of yellow and green (Figure 1). Yellow elicits positive moods and attracts the learners’ attention, while Green encourages productivity and long-term energy (Taylor, 2007). This design decision also fulfilled Principle 1, by engaging visual learners.

The final design considerations relate to the educational reinforcement mechanisms. The educational game needed to provide consequences for lessons learned during the game. This was easily introduced into “Snakes and Ladders”, as its original purpose was to teach the difference between good and evil using such mechanisms.

The Snakes and Ladders were placed randomly throughout the board, alongside information security lessons (Figure 1). Positive lessons (below ladders) provided
reinforcement by enabling ascension of the ladders. Conversely, negative lessons (above snakes) were reinforced by forcing the player to descend the board via snakes. This design associated negative consequence with negative message and positive consequence with positive message. This facilitated behaviour and knowledge patterning of multiple concepts (Principles 4 and 5).

The lesson content presented in this research’s artefact will be addressed by the next section.

3.2.2 Content. Multiple games were created for many topics, including social networking, password security and virus security. Each of the boards had a similar
design, but different content. The board, which relates to the results reported by this paper presented secure password management content. Various rules specifying the *Dos* and *Don’ts* of password security were placed above snakes and below ladders (Figure 1). The included lessons are listed in Table II.

The lessons were written as if the player had, or had not, complied with a rule of secure password management. This ‘learner-centric’ perspective serves to implement Principle 3 of the brain compatible pedagogy.

The lessons were then learnt in accordance with the rules of the gameplay which are presented in the next section.

3.2.3 Rules. “Snakes and Ladders” can be played by 2-6 players. In sequential order and starting from “Start”, each player rolls the dice and moves their representative token along the board’s sequential squares according to the number thrown. If the square a player lands on contains an information security educational message, they read it aloud and perform the accompanying action. The verbal sharing of the message helps the learners to cognitively consider the lesson (Principle 1). If the message was a “do not” lesson, they are swallowed by the snake and move their token to the square containing the snake’s tail. If it was a “do” lesson they ascend the squares ladder and place their token in the square at the top of the ladder. The first player to reach the 50th square (Finish) is the winner.

The effectiveness of this research artefact as an information security educational tool was assessed by means of experiment. The research instrument used to do this will be presented in the next section.

3.3 The research instrument

A two-part research instrument was used. The first part was a survey designed to acquire quantitative data about the learners’ information security awareness levels. They were close-ended, multiple choice questions which related to a few select lessons that were included on the board. The second part of the research instrument was open-ended interview questions. These questions aimed to gather the teacher’s perceptions of the effectiveness of the game as a teaching tool and its effect on the learner’s knowledge and behaviour.

Both parts of this research instrument were implemented alongside the research artefact in the context of the case study. This is presented by the next section.

3.4 Implementation details

For the research to be conducted, a number of evaluations were required. The implementation of these methods will be discussed in this section.

<table>
<thead>
<tr>
<th>Dos</th>
<th>Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td>You gave your password to your parent or guardian</td>
<td>You gave your password to a friend</td>
</tr>
<tr>
<td>Your password is at least eight characters long</td>
<td>Your password is less than five characters</td>
</tr>
<tr>
<td>You change your password at least once a month</td>
<td>You wrote your password down</td>
</tr>
<tr>
<td>Your password is not a word in the dictionary</td>
<td>You used your name or your pets name as a password</td>
</tr>
<tr>
<td>You used characters like !, #, $ in your password</td>
<td>You used the same password everywhere</td>
</tr>
<tr>
<td>Your password is easy to guess</td>
<td></td>
</tr>
</tbody>
</table>

Table II. Password lessons of dos and don’ts
The first step was the free distribution of the research artefact to several South African primary schools. Some of the schools targeted in the distribution were also given an introductory information security awareness talk and lesson using the research artefact. Then for the evaluation component of this research, a single class from two separate schools was selected as target group for case studies. These classes are, henceforth, referred to as Groups A and B.

Each case study involved the learners answering a pre-play survey to test their information security awareness levels for the artefact’s topic content. They were then allowed to play the game among themselves. Once the games had concluded, the learners answered the post-play survey to re-test their awareness levels. The class teachers were later also interviewed.

The research was conducted in this manner to comply with ethical research policies. To comply with the ethical research considerations of both the Nelson Mandela Metropolitan University (NMMU) and the involved schools, the researcher did not interact directly with the learners. An involved teacher from each school distributed the surveys and monitored the gameplay. The researchers later interviewed the teachers.

The results from the initial studies of Groups A and B were combined to form the pilot study for this research. The results of the study were presented within a paper presented at the Kaspersky student paper competition, and later published at WISE 2013 (Reid and Van Niekerk, 2013). The following research questions were raised as feedback from the publication:

RQ1. Can the results be replicated in other case studies?

RQ2. Is this particular game suitable for children of all age groups?

RQ3. Is the impact of the game short-term or long-term?

Based on the feedback received from these conferences, further studies were conducted. All data gathered after Group A’s initial study are, therefore, new data which were sought to confirm the findings. The resultant findings will now be addressed.

To answer these research questions, the results from the pilot were split back into their original case study groups and three new experiments were conducted. These case studies followed the same procedure as the initial studies.

The first new experiment targeted a class of older learners (12-14 years old) at the same school as the pilot group. These older learners are referred to as Group C. The initial study had already partially answered research question 1; however, this study aimed to add further evidence. It was also used to determine the answer to the second research question. It provided a comparison of the results of learners in different age ranges being newly exposed to the game.

The second and third studies aimed to determine the answer to the third research question. After a period of time, two follow-up studies were conducted to determine whether the games had influenced the learners’ long-term information security awareness. These follow-up studies were carried out with Groups A and C. Group B could not be included due to issues relating to learner availability.

Three learner groups were required to participate in these studies. The data from the original case studies were used in addition to the new case studies. The various case study learner groups and their biographical details are shown in Table III.

This section described the research artefact, instrument and implementation procedure. The next section will present the gathered data results and analysis.
3.5 Results and discussion
As discussed in the methodology section, a series of experimental case studies were conducted. These experiments involved the use of surveys as the research instrument. The gathered data are presented in subsection 4.5.1 Qualitative data were also gathered from the teachers via interview. The discussion of this data will be presented in subsection 4.5.2.

3.5.1 Research instrument results
This section discussed the results gathered from the surveys used during the case studies. The aggregated data gathered using this instrument are shown in Table IV.

Group A was the first group of children to test and play the game. Within the pre-game survey, it was found that a low majority (54.55 per cent) knew not to record their passwords; and 63.64 per cent know how to construct a strong password. Therefore, the basic knowledge of password construction and confidentiality did partially exist. However, thorough understanding of confidentiality practices, which are necessary for children, is not fully developed. Only 45.45 per cent of the learners knew not to share their password with anyone besides their parents. Overall, an initial level of information security awareness did exist. This may be partially attributed to awareness talks which had been presented to this school earlier in the year.

The post-play survey results showed a substantial improvement in the Group A’s awareness levels. The percentage of learners who answered the security knowledge questions increased in all categories. Within Group A, 90.91 per cent now knew not to record their password; 72.73 per cent now knew to only share their password with their parents; and 81.82 per cent now knew how to create a secure password. Overall, the increase in correct responses to all questions indicates that awareness was improved among the learners after playing the game. Therefore, based on these results, an initial conclusion was drawn that the brain-compatible information security game was an effective method for educating children about information security (Reid and Van Niekerk, 2013).

<table>
<thead>
<tr>
<th>Group name</th>
<th>Age range (years)</th>
<th>Number of participants</th>
<th>School</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A</td>
<td>10-12</td>
<td>11</td>
<td>School A</td>
</tr>
<tr>
<td>Group B</td>
<td>9-11</td>
<td>15</td>
<td>School B</td>
</tr>
<tr>
<td>Group C</td>
<td>12-14</td>
<td>9</td>
<td>School A</td>
</tr>
</tbody>
</table>

Table III. Participating learner groups

<table>
<thead>
<tr>
<th>Question 1</th>
<th>Question 2</th>
<th>Question 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where should you write down your password?</td>
<td>Who can you share your password with?</td>
<td>Your password should be […]</td>
</tr>
<tr>
<td>Before (per cent)</td>
<td>After (per cent)</td>
<td>Before (per cent)</td>
</tr>
<tr>
<td>Group A</td>
<td>54.55</td>
<td>90.91</td>
</tr>
<tr>
<td>Group A (return)</td>
<td>90.91</td>
<td>100</td>
</tr>
<tr>
<td>Group B</td>
<td>53.33</td>
<td>93.33</td>
</tr>
<tr>
<td>Group C</td>
<td>66.77</td>
<td>100</td>
</tr>
</tbody>
</table>

Table IV. Pre- and post-play survey results
A second test was done to corroborate the previous results. Group B, a second group of learners, was exposed to the Snakes and Ladders game. The targeted class of learners was within the same age-range but from a different school.

Within the pre-play survey, it was found that this group’s pre-play information security awareness levels closely resembled those of Group A. They too were moderately aware of secure password structure and storage practices. Additionally, their confidentiality practices were also their awareness’s weak point. Their confidentiality knowledge relating to sharing passwords was even lesser than the original test group’s, with only 26.67 per cent answering the question correctly (Group A, 45.45 per cent).

In the post-play survey, Group B, like Group A, also showed a definite increase in the number of learners correctly answering the information security awareness questions. Questions 1 (increase of 40 per cent) and 2 (increase of 46.66 per cent) indicated that the learners level of awareness about child suitable password confidentiality practices definitely increased. Question 3 also showed a definite increase in secure password creation knowledge. Group B’s results, therefore, confirm the Group A’s findings. The first research question has, therefore, been answered. Within multiple cases, playing the brain-compatible information security Snakes and Ladders game has had a definite impact on learner’s awareness levels.

Groups A and B were from the same age-range. Therefore, the conclusions drawn from their results were specific to that age range. The aim of the next experimental case study was to determine whether the game was suitable for other age groups. A study using Group C was conducted.

Results from Group C’s pre-play survey indicate that the older children also had a reasonable level of information security awareness. A moderate percentage of Group C was aware of appropriate password creation and storage principles; however, few of them knew appropriate password confidentiality practices.

Playing the game had a strong impact on Group C’s awareness levels. The post-play’s survey results indicated that all of the learners were now aware of how to securely create and store a password. The majority (88.89 per cent) also now knew not to share their password with anyone beside their parents. The results of this study, therefore, further answered the first research question, while answering the second research question. The game is suitable for raising the information security awareness levels of learners in multiple age groups.

Based on the results of these initial case studies, it has definitively been shown that the game is an effective method for raising children’s short-term information security awareness levels. The question of whether there was a long-term impact on their long-term awareness had not, however, been answered. This was the focus of the next two experiments.

In both return studies, the pre-play surveys showed that the majority of the learners, in Groups A and B, had maintained or improved their long-term awareness levels. Post-play surveys on the return studies also indicated that playing the game again raised awareness levels. Overall, these two studies indicated that the answer to the third research question is that the game has a long-term impact on the children’s information security awareness levels. This is likely to due to repeated play sessions, which maintains their awareness.
Overall, the data gathered via surveys indicate that the game is an effective information security education tool for children. These results were further supported by the teachers.

3.5.2 Teacher interview results. A secondary verification method which was used for this research was interviews with each participating class’s teacher. This section discusses the results of the interviews.

All three teachers felt that the learners had definitely learned valuable lessons, relating to the topic via the game and become more security-conscious about their personal information. Additionally, the teachers of the younger classes stated that the learners in their classes had undergone small behaviour changes, such as asking questions and reporting new findings or incidents. This indicates that the game had created higher awareness of the security issues.

All of the teachers concluded that they perceived the ‘Secure Password – Snakes and Ladders’ game to be an effective education tool.

4. Conclusion
Digital natives are constantly being exposed to information technologies and services. Consequently, they are being exposed to a variety of information security risks and threats. Therefore, information security education is a necessary life skill for today’s youth. Gameplay is proven to be an effective life skill and knowledge delivery system for the youth. Therefore, it can be used as a delivery mechanism for information security educational lessons to children.

Within the design – science paradigm, using multiple case studies, this research has shown that a traditional game-based approach, modified to include information security lessons, can be effectively used to raise basic information security awareness among learners within multiple age groups and contexts. Additionally, it has shown that that the game has long-term effect on the learner’s awareness levels and behaviour. It is, therefore, the conclusion of this author that gameplay in this format could be a viable option for the education of the future generation.

5. Limitations of research
This study had a number of limitations. First, all the learner groups who participated in this study were too small to enable analysis of findings for statistical significance. Second, the data compiled on the long-term effectiveness of the game for Group B were incomplete. This limitation was the result of School B’s ethical concerns regarding learners being a vulnerable target audience.

6. Future research
This research showed that the artefact can be used to increase children’s awareness of information security principles. However, this is not statistically proven. Providing statistically significant verification will be the aim of future research.

References


**Corresponding author**
Rayne Reid can be contacted at: s208045820@live.nmmu.ac.za

To purchase reprints of this article please e-mail: reprints@emeraldinsight.com
Or visit our website for further details: www.emeraldinsight.com/reprints
Decoding Audience Interpretations of Awareness Campaign Messages

Abstract

Purpose: This research aims to determine if the educational influence of the cyber security awareness campaign on the audience (their knowledge, behaviour and potential cyber security culture) matches the campaign’s educational objectives. The research focuses on the knowledge component of this metric by examining the awareness campaign audience’s interpretative role in processing the campaign content, through the lens of active audience theory.

Design/Methodology/approach: Using reflective practices, this research examines a single longitudinal case study of a cyber security awareness and education campaign which aims to raise awareness amongst school learners. Artefacts from a single sample are examined.

Findings: Reflexive practices using theories such as active audience can assist in identifying deviations between the message a campaign intends to communicate, and the message that the campaign audience receives.

Research Limitations and/Implications: Using this research approach, measurements could only be obtained for campaign messages depicted in artefacts. Future interventions should be designed to facilitate a more rigorous analysis of the audiences’ interpretation of all campaign messages using active audience theory.

Originality/Value: This paper applied principles of active audience theory to examine the audience’s interpretative role in processing an awareness campaign’s content based on artefacts they created after exposure to the campaign. Conducting such analyses as part of a reflective process between cyber awareness/education campaign cycles provides a way to identify areas or topics within the campaign, which require corrective action.

Paper Type: Research Paper

Keywords

Cyber security education, Active Audience Theory, Action Research, Case study, SACSAA, Reflective feedback

1. Introduction

Most awareness campaigns are dependent on the underlying assumption that the audience will not misinterpret the campaign’s message. This is not necessarily true. Measures must be taken to ensure that deviation in the interpretation of the
The importance of awareness campaigns in fostering a cyber security culture is widely acknowledged. However, many campaigns assume that the audience will not misinterpret the message that the campaign is trying to communicate. This assumption may lead to undetected miscommunications or misunderstandings. A campaign should have measures in place to check that the audience is receiving the intended message. This paper examines one possible theory that could be used as such a measure.

The importance of ensuring that cyber security awareness campaigns are successfully communicating with their audience (thereby creating a consciously cyber secure society) is directly proportionate to the growth in number of users interacting with cyberspace.

In our technology- and information-infused world cyberspace is an integral part of modern-day society. In both personal and professional contexts cyberspace is a highly effective tool in, and enabler of, most people’s daily digitally-transposed activities (Klimburg 2012; Siponen 2001; De Lange & Von Solms 2012). Several countries governments have recognized the many potential benefits that the adoption of the Internet and ICT may have for their country's welfare (Klimburg 2012). Therefore, in many of these countries, citizens are being actively encouraged to adopt these technologies. South Africa, itself has shown a rapid growth in cyber active citizen population with the tally of active internet users (cyber citizens) growing from 2 400 000 in the year 2000 to 33 464 764 users in 2015 (IWS 2015). This means that percentages of internet penetration in South Africa has grown from 5.5% in 2000 to 61.1% in 2015 (IWS 2015).

This rapid adoption of cyber technologies and services has had some very positive results e.g. providing users access to many beneficial and convenient services, utilities and opportunities for transacting, communicating, learning, socializing and many other activities. However, it has also had some negative and often unintended consequences. A prominent, problematic consequence is that the citizens are becoming increasingly technology dependent whilst also becoming increasingly vulnerable to cyber threats (Furnell et al. 2007).

Cyber users can be exposed to a wide variety of threats, examples including: Technology or hardware-oriented threats (e.g. malware, spyware, hacking), social or human oriented threats (e.g. cyber harassment, cyber-bullying, cyber stalking, social engineering attacks), content related threats (e.g. inappropriate content, illicit content, manipulated content) and finally information or risk of exposure of information threats (e.g. oversharining or incautious sharing, or accidental sharing of personal, private or otherwise valuable information). Within these threat categories numerous specialised and constantly evolving threats exist. Even highly cyber secure and aware users will never be completely lacking vulnerabilities due to the constant evolution of known and unknown cyber threats.
As the number of active cyberspace users increases, so too does the chances of a cyber threat finding a vulnerable target also increase. It is often argued that the average cyberspace citizen is not significantly aware of, or secured against, the many cyber threats targeting them. To avoid becoming victims of cyber threats these cyber citizens urgently need to acquire the security- and safety- skills necessary for safe activity within cyberspace (Siponen 2001).

All cyber users who are exposed to the risks of cyberspace must be educated about cyber security. However, this education is particularly important for children who interact with cyberspace from an early age (De Lange & Von Solms 2012; blind; Von Solms & Von Solms 2014).

It is probable that the children of the current and future generations will interact with cyberspace in many roles and capacities throughout their lifetime. These children will therefore also require cyber security knowledge and behaviours throughout their lifetime. Cyber security practices should thus ideally be considered and taught as an essential life skill for these children from the moment they begin interacting with cyberspace. Therefore, cyber security awareness campaigns and educational efforts which target children are required. These campaigns will be teaching the children knowledge and skills which will form their fundamental cyber security knowledge and skills. Therefore, it is extremely important that that these campaigns communicate their content in a manner which encourages the target audience to receive and interpret the knowledge as intended by the campaigns original content creators.

To determine whether a message is being communicated by the campaign, and received and interpreted by the audience in the way it was intended requires a measurement of some sort. Ideally the message as it was intended to be sent (the original message) should be compared to the audience member’s interpretation of the communicated message (the interpreted message). Such a comparison would provide valuable feedback, which contribute to the refinement and improvement of the campaign and its approaches. Therefore, a way to measure and compare the two messages is required. Currently little or no literature specific to the interpretation of cyber security messages exists. It is therefore necessary to examine similar problems and their solutions for other fields of study which have aimed to communicate specific messages to audiences.

Several media and communication studies have focused on similar problems. In their field the media (in various formats) aims to distribute various forms of messages. These messages can be targeted at either very broad or narrow audiences. One form of media which tries to communicate with its audience in a similar manner to an education campaign is television. Television programs (factual, or fictional) often attempt to convey specific messages and inferred meanings to their audiences. In the past the program producers, like several awareness campaign creators, assumed that the meanings of a program’s “texts” (messages) were being accepted unproblematically by their audiences (Barker 2012). However, over time they realized that this was not the case. Instead they found suggestions that the audiences...
were actively interpreting and producing meaning from the “text” within their own cultural context. The research area pertaining to this phenomenon has become known as the active audience paradigm. Within this paradigm there are a number of theories pertaining to how the meaning of the message is communicated and interpreted during the communication process between the “text” creator and the target audience.

Within the active audience paradigm (which forms part of the media and culture research area) there exists a prominent model, the Encoding/Decoding model, which was proposed by Stuart Hall (Hall 1980). This model considers the process of communicating a message as a circuit of meanings (of a text) as it goes through the process of being encoded and decoded in a communication circuit. At the end of the circuit, the model outlines a few different decoding positions an audience may fall into once they have interpreted a message that the communicator (e.g. a television show or an educational campaign) encoded and communicated. The authors believe that this model could be used, or adapted for use, in determining how a cyber security awareness campaign’s audience is interpreting the campaign’s intended message. Determining their interpretations decoding positions could assist in detecting deviations or uniformity between the audience’s interpretations of the meanings of the messages and the campaign’s intended message meanings.

To examine this theory, this paper will analyse and discuss a campaign run by the South African Cyber Security Academic Alliance (SACSAA). SACSAA runs an annual cyber awareness campaign. Its aim is to promote and instil awareness of vital cyber security and safety knowledge and behaviours within and amongst the nation’s school children. For the purposes of this research the paper will examine whether the communication of its messages to its audience is done in a way that enables the children to understand the message as the campaign’s content was intended to be understood.

This paper thus aims to use active audience theory (herein after “AAT”) as a lens, to determine whether the SACSAA Cyber Security Campaign’s target audience has been unambiguously and uncritically interpreting the meaning of the educational campaign’s awareness themes (messages) as they were intended to be communicated by the campaign’s creators. Detecting if the audience’s interpretation deviates from the campaign’s intended result may make it easier to identify necessary adjustments needed to improve the communication of content for future campaign cycles.

The remainder of this paper is structured as follows: Section 2 provides more detail about the SACSAA Campaigns. Section 3 provides a brief explanation of the AAT paradigm. The research design used to meet this papers aim is outlined in Section 4. Section 5 presents the findings of the paper. Finally, our work is concluded in Section 6.
2. The SAACSAA Campaign

The South African Cyber Security Academic Alliance (SACSAA) consists of research groups from three well-known South African Universities (SACSAA 2011). The main objective of SACSAA is “to campaign for the effective delivery of Cyber Security Awareness throughout South Africa to all groupings of the population” (SACSAA 2011). Ultimately, SACSAA intends to aid in the fostering of a societal cyber security culture via education. This paper will focus on the data gathered from the SACSAA campaign activities involving the youth. SACSAA has officially run an annual educational cyber security campaign targeting the youth since 2012 (2011 had a pilot study). The campaign consists of two components: an education campaign and a poster contest.

The campaign aims to first raise the youth’s general awareness of the need for cyber security in their digital activities. There are six main thematic messages in the campaign: “Keep your private information private”; “Be nice online”; “Stay legal”; “Trust an adult”; “Protect your PC”, “Stranger Danger”. A wide variety of cyber security and safety topics within these themes have been covered each year. These topics are presented using many modes and mediums.

Mass media is used to distribute messages and cultural forms (information) to large, widely dispersed, heterogeneous audiences (Munday & Chandler 2011). The campaign presents each topic’s content using multiple mass media modes including: digital media (awareness posters, videos, SACSAA website and online resources), printed media (awareness posters, informational pamphlets, educational games (blind) and finally public events (interactive school visits).

Each year the campaign has been modified to increase effectiveness of the successive campaign’s results and scalability. Changes and additions to the campaign have included the use of pedagogical theory, use of multimedia and interactive presentations and multimodality in the campaign material, increased contextual customization, increased teacher involvement, inclusion of SACSAA’s branding logos and mascots. Detailed discussions about the modifications and results from 2011 until 2013 are available in previous work (blind). In 2014 the campaign was adapted to be more teacher-oriented, and a cyber security school curriculum was provided. In 2015, few changes were made apart from designing the expert talks to be more automated and media centric.

The poster contest is the instrument used to measure the campaign’s effect on the involved youth’s awareness levels. Learners are invited to create and submit a hand-crafted or digital poster showing one or more awareness messages (as they understand it/them) for one or more of the campaign’s topics. They are encouraged to draw the poster as if they were teaching someone else the message. Participation in the competition is voluntarily and is encouraged through various prizes.

Evaluations of past campaign iterations’ competition posters has shown that the majority of participants have moderately or fully internalized (learned from)
campaign messages. Posters indicated internalization was: “partial” if the learner depicting the message as it was given; “moderate” if the lesson was rephrased into the learner’s own words; or “full” if the lesson was shown to be contextualized by the learner. This paper aims to determine whether the meanings of what the audience members internalised matches or resemble what the campaign objectives intended them to internalise.

Previous work has examined how the campaign has attempted to communicate messages and their meanings. The role of the audience in this communication process and their interpretive role has yet to be examined. It is the authors’ opinion that AAT could be used to understand the role of the campaign’s target audience in interpreting the campaign’s messages. The AAT paradigm is used for a similar purpose in the context of television (and other media) and culture studies, which have a similar communication intent to the campaign. The next section will examine the AAT paradigm with a focus on Stuart Hall’s Encoding/Decoding model.

3. Active Audience theory paradigm

In cultural studies dealing with television and mass media, understanding the relationship between a media “text” and its audience (audience research) is very useful (Barker 2012). In this field, the role of the audience is therefore a research focus.

There are many audience-related research areas, one of which is the audience’s role in the “consumption” of media messages or texts. Audiences can be passive consumers or active consumers. There are a number of models, which address each theoretical stance. A passive audience model assumes that a text shared by the media will have a direct, predictable influence on a passive audience. Comparatively an active audience model suggests that audiences interact with the text and actively create meaning from it based in their own cultural context (Barker 2012).

Active audience theory examines the active, interpretative role of an audience when they “make meaning” from the media content based on their own cultural context (Hall 1980; Munday & Chandler 2011). The active audience paradigm suggests that it should not be assumed that audiences develop a culture by uncritically accepting the ‘textual’ meaning of a programme (Barker 2012).

Stuart Hall’s Encoding/Decoding model suggests that an active audience has to decode the meanings within a text, therefore different audiences will do so in different ways (Hall 1980). A number of factors will influence how the audience interprets the text.

Audiences may interpret meanings from messages based on their own previously acquired cultural competencies, which they produced in the context of language and social relationships. This means that every member of an audience will have their contextual influences when they interpret a meaning from a message.
For the purpose of the encoding/decoding model an audience is considered to be a group of socially situated individuals whose “reading” of the “text” will be framed by shared cultural meanings and practices.

Stuart Hall examined the process of communicating and interpreting meaning of messages in the “conversation” between the “text” creator and the target audience.

The aim of a media “text” is typically to communicate a message with a specific meaning. The process of communication consists of a circuit of a complex structure of relations namely: production >> circulation >> distribution/consumption >> reproduction of a message (Hall 1980).

Within this circuit of communication, messages are sent between parties. Typically, the message has a meaning that the sender tries to convey when constructing and producing the message. However, as the message moves within the circuit, it is not guaranteed that each level interprets (consumes) the meaning of the message similarly. This is because the meaning of a message is polysemic (can intentionally or unintentionally have multiple meanings) and an audience can interpret these meanings in different ways. Stuart Hall’s encoding/decoding model (see fig. 1) illustrates this by showing the discourses of the meaning of the text between its producer (encoder) and the reader (encoder) (Hall 1980). Hall’s work is conducted in the context of media and culture studies.

Hall argues that media has a preferred message to communicate to their audience. The preferred message’s text would be structured and presented in a “dominance” encoding position to lead the audience to the preferred meaning (Hall 1980; Barker 2012). However this does not guarantee consumption of the encoders’ preferred meaning by the audience, as audiences do not passively accept information and its imposed meanings from a structured ‘text’ (Munday & Chandler 2011).

**Figure I: Meaningful Discourse (Hall 1980)**

Within the circuit of communication the encoding/decoding model shows that audiences are active and knowledgeable producers of the meaning of a text’s delivered message within their personal and social contexts (Barker 2012). The producer (encoder) encodes meaning in a certain way, while the reader (decoder) decodes it differently according to their own personal knowledge and contextual frames of interpretation. It cannot be assumed that the meaning of a program, text or any other communication has a fixed interpretable meaning, which can unerringly be recognized by any audience. Instead how the audience makes sense of a text’s meaning is “the product of a negotiation between the audience and the text in a particular context of reception” (Munday & Chandler 2011).
The audience and the producers/encoders of a message are expected to share the interpreted meaning position to the same degree that they share cultural codes (Barker 2012). To increase the amount of shared meanings it is therefore very important when developing material or communicating a message that it be developed or communicated to try apply and leverage similar or shared social situated knowledge and practices in the communication of the messages.

In brief, different audiences (and the encoders) may accept different textual meanings, based on how the text is constructed and communicated, and based on their contextual cultural influences. Texts (the messages) are polysemic (can have multiple meanings)(Hall 1980). Often only some of the meanings will be accepted by an audience (Barker 2012). The audience’s decoding will typically fall into one of the following three hypothetical decoding positions as proposed by Hall:

1. “The dominant-hegemonic encoding/decoding” position - where the decoder accepts the messages “preferred meanings” which a text is attempting to impose (Hall 1980). Often this position is adopted as the text usually reflects the ideas and beliefs of the audience e.g. the subject matter may be the reason or relate strongly to a reason the audience member is interested matter or it may affect their life or activities to some degree;

2. “A negotiated code” position - wherein the decoder acknowledges the legitimacy of the theory of the hegemonic decoding, but adapts its interpretation based on particular circumstances or context (Hall 1980). This position is adopted when an audience member understands the meaning of the text, but it doesn’t relate to them in a degree of interest which would motivate them to further decode its meaning e.g. the audience member may acknowledge the importance of a concept but since they do not need to apply it in their lifestyle of activities they may not require knowledge of specific details etc.;

3. “An oppositional code where audience members understand the preferred encoding may reject it and decode the text in contrary ways” (Hall 1980). In this position, an audience member consciously rejects the preferred meaning, and/or consciously or unconsciously relates to an opposing view. For example, the text’s message provides the positive information about a particular issue; however, the audience better relates to the negatives of the same issue.

All positions are the result of the whole communication process and the audience members’ decoding of the text in order to produce their own meaning of the message.

The campaigns make use of a variety of mass media to communicate. Additionally, the campaign and mass media have similar intents of communicating a message with a preferred meaning or interpretation. Consequently, the authors believe it is possible to use the encoding/decoding model to analysis an awareness campaign’s audience’s interpretation of a campaign’s messages. Therefore, the next section will outline how to conduct such an analysis.
4. Research design

This section presents the research design for how Hall’s encoding/decoding model could be used in an analysis of the SACSAA’s campaigns audience’s interpretation of its messages. Determining the decoding position espoused by the majority of the SACSAA audience’s takes, could indicate what elements of the campaign are successfully, or unsuccessfully, meeting campaign objectives. In addition, it could indicate in the long-term what type of culture the campaign is encouraging to develop.

The annual SACSAA educational campaign has been running since 2011 as a longitudinal case study. Its intended long-term target audience is all South African youth. However, thus far data has only been gathered from the numerous schools in the Nelson Mandela Metropolitan area who have been increasingly exposed to the campaign. The campaign aims to contribute to the fostering of a cyber security culture through the education of the youth. This paper aims to determine whether the targeted youths’ understanding of the cyber security messages delivered, matches the objectives of the campaign and will thus have the desired cultural effect. Part of the campaign’s enhancements over the years has been the customization of the material to fit the issues of each particular school. Therefore, in order to measure an effect on an audience and its culture it would be best to examine one particular audience and context i.e. one school which has been exposed to the campaign for several successive years. Therefore, for the purposes of this paper only data gathered from the single school which have participated in every campaign since 2012 until 2015 (last complete campaign) will be used. This school will be referred to as ‘School A’.

The campaign data used in this study was gathered prior to the conceptualization of this paper’s research topic. In fact, it was the authors’ perception of certain messages being misinterpreted by the audience in this campaign that lead to an investigation into theories that could be used to measure such misunderstanding. Therefore, the data gathering instrument and parameters were not specifically designed for this research report. The data used, is relevant to the study, however it may not be as complete as it could have been had the data gathering process been designed specifically for this research’s purposes. Future research will make use of customised research design and implementations procedures and instruments to gather a more complete and suitable data set.

‘School A’ is a convenient and purposive sample for the analysis purpose of this paper. Firstly, it is a convenience sample as the data was “available to the researcher by means of its accessibility” (Bryman 2012). The researchers have been gathering data for a number of successive years for research purposes. Secondly, this sample is also purposive as the sample participants were specifically selected "so that those sampled are relevant to the research questions that are being posed” (Bryman 2012).

Over the years the campaign material and approach has altered and improved. These changes were implemented for a variety of reasons, including: to improve the effectiveness of the campaign; to create brand awareness, to increase message
internalization and address previously identified campaign faults or research gaps ((blind,blind,blind,blind)). This paper’s research examines the audience’s interpretations of campaign’s content. The changes in measurements of the audience’s interpretations, acceptance or rejections of the content may have been influenced by the changes made to the campaign overtime. Therefore, the changes made over within each research cycle will be briefly outlined in Table I.

**Table I: Changes or adjustments made to annual cyber security awareness campaign**

The students within ‘School A’ have been exposed to all of the involved culture fostering and measurement activities and have thus been exposed to all the various adaptions made to the campaign. The sample is believed to be representative of the SACSAA campaign’s general target audience’s primary school subgroup for the following reasons: the participants are all primary school children; their age ranges between 6 and 15; members of both genders participated; and different ethnic groups were represented. Due to ethical considerations no identifying data apart from participant age was captured.

A content analysis; as described by Krippendorff (2004); was done to determine if the audiences interpretation of the material aligned with the subject-expert and educator’s intended key messages for each campaign topic. A content analysis can be conducted on texts and artefacts (Hodder 1994). The posters submitted by learners to the SACSAA campaigns competition are considered to be texts and artefacts. They illustrate how each learner understood the campaign’s messages and how they had interpreted them.

The researchers consider the SACSAA competition posters to be iconic cultural artefacts, which provide information about the culture of their creators. Therefore, the analysis was conducted on the competition posters gathered from ‘School A’. The aim was to determine if the learner’s interpretation of the educational message matched, closely related. The interpretations could be aligned to one Hall’s three decoding positions depending upon whether it generally agreed with minor differences in interpretation, or opposed the campaign’s intended meanings. For the purposes of this paper, a fourth decoding position could be “null” wherein where the audience members did not understand/accept/process the message clearly enough to take any of the above positions. This additional position is deemed necessary due to the very young age of some members of the specific campaign’s intended audience.

For this analysis the following questions were asked for each poster: Firstly, “What topic(s) do the message(s) in the poster cover?” and secondly, “What position within Hall’s encoding/decoding theory did the audience member (poster creator) take once they decoded the campaign’s message (in the researcher’s opinion)?” Each of these questions and the analysis process for answering them will briefly be elaborated upon in the next two subsections.
4.1. Posters per topic

This question was to determine which specific topics were considered more important or accepted more readily by the learners. The campaign covered all of its topics well, however, it placed emphasis (considerable content) on the issues it considered critical issues. These thematic issues messages are: promoting anti-cyber-bullying, personal pc and information protection, and staying legal online. The percentage of posters covering a topic will be compared to the ratio of the campaign’s content which covered the topic. The difference between the percentages could indicate a match or difference between the audience’s and campaign’s rating of importance for the covered issues.

4.2. Poster creators decoding position on the related campaign topic’s message (according to Hall’s encoding/decoding theory)

This question was asked to determine if the way the participant interpreted the message of the material aligned with how the campaign intended it to be understood. The participant’s interpretation of the campaign topic(s)’s message(s) (as the show it in their poster) was categorized as having one of the following positions: the dominant-hegemonic decoding position; a negotiated coded position; or an oppositional coded position. These positions meaning according to Stuart Hall are explained in Section 3. In order to determine which of these positions a poster belonged to, the following questions were asked as an evaluation matrix:

1. Does the posters **textual message** support the related campaign topic(s) message?
2. Does the posters **graphical message** (examples/warnings) support the related campaign topic(s) message?
3. What overall impression (in the researcher’s opinion) does the poster give of the participant’s interpretation of the related campaign topic(s) message?

The answers to these questions were selected to be one of the following: strongly supports related campaign topic’s message; partially/vaguely supports related campaign topic’s message; opposed related campaign topic’s message; undeterminable. If two or more questions were answered as strongly supporting the related campaign topic’s message, the poster was classified as having accepted the dominant-hegemonic decoding interpretive position. Likewise, if two or more questions were answered as strongly opposing the related campaign topic’s message the poster was classified as having accepted an oppositional coded interpretive position. Other combinations of answers resulted in the poster being classified as having accepted a negotiated coded interpretive position, unless two or more question was answered as ‘undeterminable’ in which case the posters was classified as having a “null” or “undetermined” position. “Null” position posters were typically considered impossible to interpret without further information. An example of the results of using this matrix may for classification purposes is shown by Figure II.

An example of a poster which is categorised as accepting the dominant-hegemonic (preferred) encoding/decoding of the campaign’s message for the topic of cyberbullying is shown in Figure IIa. The text strongly supports prevention and
stopping of cyber bullying and provide tips on how to do this. The graphics strongly support the message e.g. it shows the consequences (emotional pain) of the cyber bullying on the victim and the platforms this bullying may occur on. Overall the poster strongly suggests that the participant agrees with the campaigns objective of promoting the prevention of being a cyber-bully and/or victim of cyber bullying.

In contrast to Figure IIa, Figure IIb shows an example of a poster which is categorised as representing an oppositional coded interpretative position for cyber bullying topic. The textual message was classified as being oppositional as it did not discourage cyber bullying in anyway, instead it seemed to say cyberbullying is inevitable and consequences should be disregarded. The graphical pictures illustrated an example of cyber bullying but did not indicate it should be stopped or that it was bad, therefore they were also classified as being oppositional. Overall the poster seemed to promote cyber-bullying rather discourage it.

Figure II: Examples of classification of poster interpretation positions

As discussed in the introduction, measuring the audience’s decoding position concerning the meaning of the subject depicted in their posters fulfils the purpose of this research by determine if the educational influence of the cyber security awareness campaign on the audience’s cyber security knowledge and awareness levels matches the campaign’s educational objectives.

The remainder of this paper will discuss the results of the quantitative analysis. It will then conclude with the papers findings in terms of its aim.

5. Analysis and results

This analysis aims to determine whether the messages received by the audiences match the campaigns intended messages and thereby helps to foster the desired culture. This section will firstly present the general information about School A’s submissions. Then it will present discussions of the results of the analysis of the submissions based on the AAT analysis matrix previously discussed in Section 4.

The analyses conducted cover the all of the posters submitted each year. Excluding the pilot study year, School A has participated in every SACSAA cyber awareness/education campaign and competition. In total, from 2012 through to the 2015 campaign, School A has had 362 learners voluntarily, and successfully participate in the SACSAA poster completion. Figure III shows the participation numbers for each year. Over all the school’s learner participation tally has shown a positive trend of growth.

Figure III: Learner participation per year
The next two subsections will conduct the analyses on the data gathered from these posters.

5.1. Analysis of posters per topic per annum

This section discusses the analysis of the percentage of total posters which depicted the messages of the campaign topics for each year. The poster competition required one or more message/s or topic/s to be covered within their poster entry. This analysis will reflect which topics audiences consider important. Figure IV shows the historic percentage tallies of how many posters covered each topic’s messages each year. Most of the posters through the years have had covered singular themes or topics, however some posters have address multiples. The percentage of each year’s posters which covered multiple topics each year are as follows: 2012 – 14%; 2013 – 38.24%; 2014 – 16.67%; 2015 – 15%.

Based on Figure IV, posters have constantly reflected that learners strongly consider the topics of “cyberbullying”, “information/password security” and “Virus & Malware” or particular importance. Contrastingly they show almost no regard for the topic of “Piracy” particularly the material view of promoting “anti-piracy” messages. The remainder of the topics had varied states of depiction over the years.

Figure IV: Percentage of posters covering a topic’s messages per annum (%)

These four messages were all strongly focussed on as serious issues in all of the campaign material, as they are issues which are strongly associated to children’s cyber activities. The audience seems to agree with the campaign about the importance personal and asset security and safety. These benefit from this knowledge and associated practices. However, they reject the campaign’s view that piracy and infringement of others individual’s/entities property rights should be stopped (particularly if they benefit from the infringement).

5.2. Analysis of the decoding positions indicated by the campaign audience’s posters each year

This analysis examines which interpretive position based on the AAT matrix, the participant’s posters indicate the learners have taken. For the topics which have been depicted in the posters, this measurement could indicate whether the audiences and the campaigns interpretations of the message meanings are synching or deviating. Figure V displays the percentage of posters (learners) per AAT decoding position within each topic category for which they had depicted a message. Using Figure V the remainder of this section will discuss the finding in terms of the AAT decoding positions.

Figure V: Percentage of Posters in per AAT position each year (%)
5.2.1. “The dominant-hegemonic encoding/decoding”

The topics which have consistently had this decoding each year are: Stranger Danger, Social Networking, Cyberbullying, Cyber Citizenship, Cyber Crime and Information/Password security. Other topics which have had high depiction rates but have fluctuated yearly are: Browsing and downloading (2012, 2013, 2015); Danger of online activities (2013, 2015); Hardware security (2013-2015). Piracy was the least depicted topic and never showed a dominant interpretation.

When the campaign has large quantities of posters in this decoding position it indicates that although there is some room for improvement (until it is 100%), this message does have message text’s which are being successfully communicated. This interpretation could be held for the following reasons: firstly, they are very relatable and relevant issues for the target audience; and secondly, it is extensively covered by the material.

The contributions of the material coverage and customisation can be controlled by the campaign creators. Therefore, lessons from the topics presentation and communication from the years they were most dominantly interpreted should be applied to these and other topics. E.g. Cyberbullying and stranger danger (including social network aspects) were the most requested customizations for the expert presentations at the school.

5.2.2. “A negotiated code” position

The majority of the posters overall in every category were negotiated to some degree. Frequently they almost adopted the preferred meaning, however they had a margin of contextual interpretation from the learner’s perspective which prevented the depicted message from perfectly aligning with the campaign’s preferred message meanings. The majority of these poster creators could be persuaded to accept the campaigns preferred meaning after further or more in-depth exposure to the campaign.

5.2.3. “An oppositional code”

Over the past few years there have been topics which had oppositional interpretation depicted in posters. The topics per year are as follows: 2012(None); 2013 (Stranger Danger, Browsing and Downloading); 2014 (Stranger Danger, Cyberbullying) and 2015 (cyberbullying, information and password security, viruses and malware, piracy). These messages were all strongly covered in the campaigns. The posters which indicated this interpretation seemed to illustrate the situation but did not indicate that any of the negative issues within the topic should be prevented, or supervised. Several of the poster classified as being oppositional actively encourage the opposite of the campaigns preferred meaning for the message text. These topics will require communication adjustments to try prevent the oppositional view from being taken.

This section provided the general context and facts about the learner’s participation in the campaigns poster competition. Then it conducted analyses to answer the first
research design’s questions: “What topic(s) do the message(s) in the poster cover?” in section 5.1; “What position within Hall’s encoding/decoding theory did the audience member (poster creator) take once they decoded the campaign’s message (in the researcher’s opinion)?” in section 5.2.

A limitation the analyses is that measurements could only be taken for the topics a messages which the audience depicted in their posters. Other messages and their meanings may have been relatable for and accepted, negotiated or rejected by the audience, however within the current research design they could not be measured or analysed. The next section will outline the final conclusions of the paper.

6. Conclusion

The use of AAT as a lens of analysis of the audience’s interpretations of the campaign messages, in the context of the SACSAA campaign, was very successful. It assisted in identifying whether each annum’s campaign and audience had intended or interpreted meanings for corresponding campaign messages which were comparatively uniform or deviated.

The majority of the campaign’s audience has been actively producing meaning from the materials messages. The majority of the audiences have been consistently decoding the meanings of each annum’s campaign’s messages in the dominant-hegemonic (preferred meaning) position. Additionally, the majority of the remaining audience members have been interpreting the materials meaning in the negotiated coding position. The majority of the audience numbers who have a positive or acceptable negotiated interpretation of the relevant campaign message’s meaning.

These findings were particularly strong for messages which strongly related to the participants perceived personal/asset security. However, the findings also indicated that the audience preferred to negotiate or reject messages that they did not perceive to have a negative consequence for themselves e.g. messages relating to piracy.

Overall, this paper concludes that the majority of the campaign messages are being heard, and subscribed to by the target audience. Consequently, if a cyber security culture is developing amongst this audience, it matches the culture which the campaign material intends to foster. This outcome could further improve, if future work establishes how to encode material to encourage audiences to accept the campaign’s less preferred messages.

Future research and campaign implementations should conduct an analysis using the encoding/decoding model’s concepts as part of a reflective feedback process which could contribute to the improvement or maintenance of the campaign.

7. References


<table>
<thead>
<tr>
<th>Campaign Year</th>
<th>Changes/adjustments made to campaign</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>• Pilot study</td>
</tr>
<tr>
<td></td>
<td>• Distance learning campaign</td>
</tr>
<tr>
<td></td>
<td>• Informational pamphlets were distributed for topics of interest</td>
</tr>
<tr>
<td></td>
<td>• Participants were required to self-motivate and self-study given and additional materials.</td>
</tr>
<tr>
<td></td>
<td>• Cash prizes were offered for the competition winners</td>
</tr>
<tr>
<td>2012</td>
<td>• Self-study requirements were reduced</td>
</tr>
<tr>
<td></td>
<td>• A researcher or subject expert gave a formal informational talk at the schools. The presentations were customised to include example within topics which were more relevant to the addressed learners and audience age-groups.</td>
</tr>
<tr>
<td></td>
<td>• Pamphlets, and additional online SACSAA reinforcement materials including cyber security games were provided to the schools</td>
</tr>
<tr>
<td></td>
<td>• Brain-compatible education pedagogical principles were applied to all materials and educational experiences.</td>
</tr>
<tr>
<td></td>
<td>• A campaign mascot (Cyber Sid) was introduced</td>
</tr>
<tr>
<td></td>
<td>• Generous (non-cash) prizes were offered for the competition winners</td>
</tr>
<tr>
<td>2013</td>
<td>• A researcher or subject expert gave a formal informational talk at the schools – the presentations were customised for each school. Teachers could pre-request more detailed discussions about topics they knew were affecting learners at their school.</td>
</tr>
<tr>
<td></td>
<td>• Pamphlets, and additional reinforcement materials including cyber security games were provided to the school’s teachers to use in other lessons or follow-up discussions. These material were also customised for each school.</td>
</tr>
<tr>
<td></td>
<td>• Teachers were asked to encourage student participation in the competition.</td>
</tr>
<tr>
<td></td>
<td>• The brain-compatible education pedagogical principles were applied to all materials and educational experiences.</td>
</tr>
<tr>
<td></td>
<td>• The Cyber Sid mascot was replaced by the SACSAA logo on all the provided material</td>
</tr>
<tr>
<td></td>
<td>• Generous (non-cash) prizes were offered for the competition winners</td>
</tr>
<tr>
<td>2014</td>
<td>• A researcher or subject expert gave a formal informational talk at the schools – the presentations were extremely customised and contextualised for each school. Anonymised stories (from the context of the schools) which had been provided by teachers were included in the talk to increase relatability and relevance for the target audience.</td>
</tr>
<tr>
<td></td>
<td>• Pamphlets, and additional online reinforcement materials including cyber security games were provided to the school’s teachers to use in other lessons or discussions.</td>
</tr>
<tr>
<td></td>
<td>• Teachers were asked to encourage student participation in the competition.</td>
</tr>
<tr>
<td></td>
<td>• Teachers were provided a complete, customisable cyber security education curriculum for the various age-groups. Additionally, they were invited to a workshop where they were provided training for the use of the curriculum.</td>
</tr>
<tr>
<td></td>
<td>• The brain-compatible education pedagogical principles were applied to all materials and educational experiences.</td>
</tr>
<tr>
<td></td>
<td>• Both the Cyber Sid mascot and the SACSAA logo were used within provided material</td>
</tr>
</tbody>
</table>
- An additional campaign mascot (Cyber Sindi) was introduced to be inclusive of both genders
- Generous (non-cash) prizes were offered for the competition winners

2015

- A researcher or subject expert gave a formal informational talk at the schools – however the talks were changed to reduce the expert’s speech and increase the amount of media (videos, infographics, etc.) within the presentations. The customisation of the presentations was less extreme than the previous year, returning to 2013’s levels of customisation.
- Both mascots, Cyber Sid and Cyber Sindi mascot as well as the SACSAA logo were used within provided material
- The campaign was run at a later time in the academic calendar
- The remainder of the campaign was identical to the previous year excluding the running of a teacher’s workshop.
Figure I Meaningful Discourse (Hall 1980)
232x82mm (96 x 96 DPI)
Figure II Examples of classification of poster interpretation positions
165x69mm (96 x 96 DPI)
Figure III Learner participation per year
127x73mm (96 x 96 DPI)
Figure IV Percentage of posters covering a topic's messages per annum (%)
Figure V Percentage of Posters in per AAT position each year (%)  
216x148mm (96 x 96 DPI)
Appendix B: Conference publications stemming from this thesis
Cyber Safety for School Children
A Case Study in the Nelson Mandela Metropolis

Abstract. Protecting the youth against the dangers posed by cyber space has become a matter of national priority. Parents often lack the necessary cyberspace know-how, to teach their own children how to be safe online. It has thus become the responsibility of society at large to educate the youth. This paper reports on a cyber safety poster creation campaign in the Nelson Mandela Metropolis in South Africa.

1 Introduction

For many nations, protecting the youth whilst they use cyber space, has become a matter of national importance. The UK National Cyber Security Strategy [1, p. 26] list ”to tackle cyber crimes like online bullying...” as one of its ”priorities for action”. Klimburg [2] provides an overview of more than 20 National Cyber Security Strategies (NCSS), and notes that ”Cyber security at the national level will fail when there is an inappropriate level of cyber security awareness and education” [2, p. 133]. Such awareness and educational campaigns should include all members of society and should range from primary and secondary school level, to awareness campaigns aimed at adults and the elderly [2].

The protection of national interests in cyber space has received a lot of focus in recent years. More than half of the NCSS examined in Klimburg [2] were introduced since the start of 2011. In fact, the international standard ISO/IEC 270032 [3], which differentiates cyber security from other forms of security, was first published in 2012. To a large extent, this urgency to address cyber security related issues stems from the speed with which use of the World Wide Web have diffused through society.

The technology that makes the World Wide Web possible was first created by Berners-Lee in 1990 and the first Web server became operational in 1991 [4]. Today, barely two decades later, an estimated 2.4 billion people uses the Web on a regular basis [5]. Use of the Web has permeated every aspect of many people’s daily lives. The Web is used to play games, to do research, to conduct business, to perform personal financial transactions, and for many other daily tasks. Unfortunately the adoption and diffusion of many technological innovations often have undesirable and unanticipated consequences [6]. One of the unanticipated consequences of the diffusion of the Web, is that the parents of the current generation of children using the Web mostly grew up before the Web existed. These parents are thus ill equipped to teach their children how to use the Web safely. It
has thus become the responsibility of society at large to try to create awareness amongst children regarding the dangers posed by cyberspace.

This paper presents a case study of a cyber safety awareness campaign conducted amongst school children in the Nelson Mandela Metropolis. The researchers hosted a cyber safety awareness poster creation competition as part of a larger national cyber security awareness week. This paper presents the lessons learned during this campaign and also discuss some interesting observations made by the researchers during the campaign.

2 Methodology

The paper is structured according to the guidelines for a Case Study as presented by Creswell [7]. Creswell suggest the following structure:

- Entry vignette
- Introduction
- Description of the case and its context
- Development of issues
- Detail about the selected issues
- Assertions
- Closing vignette

In the context of this paper, the abstract and introduction to the paper respectively serves as the case study’s entry vignette and introduction. The next section will describe the case and its context.

3 Description of the case and its context

The South African Cyber Security Academic Alliance (SACSAA) was formed in 2011 by researchers from three South African universities, namely the University of Johannesburg (UJ), the University of South Africa (UNISA), and the Nelson Mandela Metropolitan University (NMMU). “The main objective of SACSAA is to campaign for the effective delivery of Cyber Security Awareness throughout South Africa to all groupings of the population” [8].

As part of its cyber security awareness activities, SACSAA hosted South Africa’s first national cyber security week in October 2012. Preparations for this first national cyber security awareness week started in 2011. The initial plan was to host such a week in 2011. However, due to logistical reasons it was decided to postpone the first national week to 2012. Each of the three founding institutions committed to conducting at least one major cyber security awareness initiative as part of the activities for this national event. The NMMU researchers decided to host a cyber security awareness poster creation competition. This poster competition forms the focus of this case study. The case study will present a brief overview of the hosting of this competition and will report on the lessons learned by the researchers conducting this event.
4 Development of issues

A 'trial run' of the planned poster creation competition was held in 2011. This was followed in 2012 by the first fully fledged competition. The following subsections will briefly describe how the hosting of the ‘trial run’ differed from the first fully fledged awareness competition in 2012.

4.1 The ‘trial run’ in 2011

The 2011 ‘trial run’ started in the 3rd term of 2011. During this term hundred of professionally created and printed promotional flyers which advertised the competition was distributed via ‘snail mail’ to schools in the Nelson Mandela Metropole. Flyers were also posted on noticeboards across the NMMU campus. Figure 1a shows an example of the 2011 competition flyer.

![Competition Advertising Flyer](image1.png)  
![Cyber Safety Pledge](image2.png)

Fig. 1: Examples of material distributed to schools.

The 2011 ‘trial run’ called for entries in the form of either awareness raising posters or videos. The posters could be submitted in either digital form or physical copies could be mailed as entries. The competition asked for entries in one of three categories, namely:

- A primary school division
- A secondary school division
- An open school division, which anyone could enter, irrespective of age
The competition offered cash prizes to the winners. These prizes were reasonably generous in the South African context.
Despite a lot of effort in the advertising of the contest during this year, only three posters and one video was received as entries for this 'trial run' competition.

4.2 The first 'official' competition in 2012

In 2012 the first 'official' competition was hosted as part of the national cyber security awareness week. A lot of effort went towards not repeating the mistakes that were made during the previous year’s 'trial run' competition. The following changes were made:

– The printing and distribution of flyers to call for participation in the competition was printed during the first term of the year and immediately distributed. This was done because many school teachers who received flyers via the mail the previous year responded with concern that the third term was too late in the year for them to meaningfully encourage learners to participate.
– The competition was more focused. Only poster entries was called for and the previous year’s video category was removed.
– Entries was restricted to the school children only. There was thus just a primary school and secondary school division call. The previous year’s open division was removed because the researchers felt that this category did not meaningfully contribute to the actual raising of awareness amongst the entrants.
– The researchers visited several schools and delivered competition flyers in person. Whilst delivering these flyers effort was made to explain the context and purpose of the competition to the teachers involved.
– Following the hand delivery of competition flyers the researchers were invited to present cyber security talks at some schools. During these talks copies of an awareness flyer developed by the researchers entitled "Cyber Safety 101" were distributed to teachers and participating learners. These awareness flyers are discussed in depth in a later section.
– The competition received radio and media exposure as part of the larger national cyber security awareness week campaign. Following this exposure, many sets of competition flyers and accompanying basic awareness flyers were distributed on request to schools in several provinces.
– The competition were supported by the activities of other SACSAA member institutions. Of specific interest to this case is the distribution of a cyber security pledge form to learners in participating schools. This pledge form was signed by learners and signified that they pledge to 'surf on the safe side'. The pledge form listed three promises which all reinforced specific messages that also formed part of the messages on the "Cyber Safety 101" flyers. The pledge form and other awareness material distributed as part of the larger national campaign were branded with a 'mascot’ in the form of a robot figure with a lock on its chest. The pledge form is depicted in Figure 1b.
The 2012 campaign was a lot more successful than the trial run in 2011. A total of 217 poster entries were received. Of these entries 94 were from primary school children and 123 were from secondary school children. However, despite having many requests from schools located all across South Africa for competition flyers, educational material and additional information regarding how to enter, all entries received were from the Nelson Mandela Metropolitan area. In fact, all entries were received from schools that were visited in person by a member of the research team to advertise the competition and explain its purpose to learners and teachers.

The following section will provide more detail regarding the awareness message gave during our visits at schools and will present the results of a content analysis performed on the poster entries received.

5 Detail of selected issues

5.1 Educational Flyer

During the initial 'trail run' in 2011 many teachers who were asked to encourage their learners to participate stated that they do not know enough about cyber safety and/or security to give advice to children regarding poster topics. This lead to the creation of an educational flyer by the researchers to be send to schools with the 2012 poster contest flyer. The flyer list seven basic cyber safety 'rules' that children can follow to help them stay safe online. The contents of this flyer also formed the basis of the cyber safety talks presented at the schools by the researchers.

The following is a verbatim copy of the listed 'rules' on this flyer:

1. Protect your computer - As a minimum every computer should run an antiv
  irus program and a firewall. Very good antivirus and firewall software is
   available free of charge. Visit our website for more info.
2. Have a good password - A good password should contain UPPER and lower
   case alphabetic characters, numbers, and some special characters. Try using
   the first letter of every word in a sentence combined with a few twists like
   using the last word in full. For example: My name is Bob and I like to eat
   = MniBall2e@t.
3. Never share personal details online - One of the biggest online dangers is
   that criminals can find your personal information like your ID number, date
   of birth, address, or cell number and use it to steal your identity. Never post
   either your own, or anyone else's personal information online!
4. Dont trust anyone online - People you meet online are rarely who they say
   they are. Never believe that someone you met online is telling you the truth.
   Be especially wary of gifts, competitions, and other prizes. How can you win
   if you never entered?
5. Dont break the law - Illegal software, games, or music often contains hidden
   malware. Why would someone go through all the effort to crack the copy
   protection on a file if there is nothing in it for them?
6. Don't be a bully - Everything you post online stays there forever, even if you delete it. Do you really want the people you are going to work for one day to know how nasty you were to someone else today?

7. Trust someone - It is a good idea to have at least one adult you can trust who knows who you are talking to online and what you do when you are online. This could be a parent, uncle, aunt, teacher, or even a brother or sister.

The above mentioned flyer was handed out at all schools that were visited in person during 2012. Schools that requested that additional information be mailed to them via 'snail mail' also received copies of these flyers. Due to available time and logistical issues, schools that were initially visited and invited to participate did not receive copies of these flyers unless they were also visited a second time for the researchers to present a cyber safety talk to the learners.

5.2 An Analyses of the Poster Entries

All 2017 poster entries in the 2012 competition came from only four schools, one was a primary school with most learners between the ages of 6 and 13 years of age. the remaining three were secondary schools with learners predominantly aged between 13 and 18 years old. All of these schools were amongst those visited in person by the researchers. However, only the primary school received a cyber safety talk and the accompanying copies of the "Cyber Safety 101" flyers. In all cases the researchers were contacted by the teachers of the entrants and asked to collect the poster entries for the entire school in a batch. The primary school children thus each had a copy of the topics suggested by this flyer, whilst the secondary school children’s entries were primarily based on their own, or possibly their teacher’s, perceptions of what would be relevant topics.

The authors performed a qualitative content analyses on all the poster entries that were received. For this analyses the following questions were asked for each poster:

1. What topic(s) is covered by the message(s) in the poster?
2. Is the poster specific to one category (form factor) of device?
3. How well has the cyber safety message been internalized (in the researchers opinion)?

Each of the above questions will be briefly elaborated on in the following sub-sections.

Posters per Topic This question was asked to firstly determine how well the message contained in the "Cyber Safety 101" flyer was received by the learners. Secondly the researchers wanted to know which specific topic(s) was seen as more important by the learners and whether or not there was a difference between the topics primary school children and secondary school children considered important. Figure 2 shows the results of this part of the analyses. As can be seen
in Figure 2 the primary school children predominantly based their posters on messages contained in the "Cyber Safety 101" flyer, whilst the secondary school entries also included the topics of social networking, phishing, and identity theft. Secondary school entries on the "Protect your computer" topic also covered a much wider range of malware and were not restricted to anti-virus or firewall related messages, which most primary school entries were. Of interest to the researchers was that the most popular messages for primary school children was to not trust strangers, or give out personal information online. For secondary school learners not to be a cyber-bully was by far the most popular message. Very few children chose the message that related to not using illegal software or media as the topic for their posters.

![Fig. 2: Number of Posters per Topic](image)

Also of interest to the researchers was that many (20 out of 94) of the primary school posters used the robot 'mascot' in the poster design. In many cases where the robot was used as a motive the message stated that the robot will help protect you against the dangers of cyber space.

**Posters per Category of Device** The purpose of this question was to determine whether the children associated the Web with a more ‘traditional’ computer, or with a mobile device, or whether they made no distinction between computers and mobile devices like smart-phones. The results of this analyses is shown in Figure 3. From this analyses it appears that the primary school children tend to associate Web use with a single device whilst secondary school children don’t make such a distinction.
**Internalization of Cyber Safety Message** The final question asked in the analyses attempted to judge how well the child internalized the message(s) portrayed in the posters. If the poster just re-iterated a message from the flyer in more or less the same words as it were given to them it was rated as "As given", if however the message was expressed in the child's own terms it was rated as "Rephrased in own terms", finally if there was clear evidence that the child also understood the implications and/or consequences of not adhering to the message’s advice it was rated as "Fully internalized". An example of a poster considered "Fully internalized" is depicted in Figure 4. In the poster shown in 4 one can clearly see how the child interpreted the concept of cyber-bullying. A character called Sam send an untrue message claiming "Jo said she likes Mike". Jo is crying because she never said this and Mike is confused because he was unaware the Jo likes (has a crush on) him. The poster shows that the child understood false messages about other to be cyber-bullying; she also understood that such action could hurt others, hence Jo’s tears, and by showing the same message on all depicted character’s devices she demonstrated that she understands that such bullying is often via a public forum and not limited to one-on-one communication.

An initial analyses compared primary to secondary school children. However, it was found that almost all the secondary school entries was rated as "Fully internalized". The primary school sample was then sub-divided into children aged 6 to 9, and those aged 10 to 13 for a secondary analyses. This analyses, as depicted in Figure 5 showed that the younger children internalized the safety messages to a lesser degree than the older group.
6 Lessons Learned

During the 2012 poster competition the researchers have learned many lessons, which can hopefully assist to make similar campaigns in future more successful. The following is a brief summary of the lessons learned:

1. Schools will only participate in campaigns like these if they are notified of the campaign early in the year.
2. Personal visits to schools are a lot more effective than mailed invitations - No entries were received from schools that were not visited in person. Even schools that specifically requested entry information via the mail did not participate.
3. Teachers play a vital role in such campaigns and need to understand the relevance of the campaign.
4. Prizes should be distributed across many categories. - Initially the researchers planned to have prizes split into only two categories, namely primary and secondary school categories. However, many primary school teachers expressed concerns that it would not be fair to judge/compare poster entries by 6 year olds against those entered by 13 year olds.
5. Guidance regarding judging criteria should be specific enough to ensure desired outcomes. - The intention of the poster creation campaign was to use the best poster entries received as awareness raising posters in future campaigns. Unfortunately a lot of the entries has a lot of text and were in the format of informational brochures, rather than that of awareness posters.
6. Mascots and other branding should be chosen with care. - Children do relate the mascots to the topic.
7. Hand drawn or painted entries should be encouraged. - The majority of entries created with the aid of a computer were of a 'cut and paste' nature. The researchers believe that the hand drawn posters provided a better indication of actual assimilation of the subject matter.

## Conclusion

Protecting the youth in cyber space has become the responsibility of society at large. Without an appropriate level of cyber security awareness and education national cyber security strategies cannot work. This paper reported on a cyber safety awareness campaign conducted in the Nelson Mandela Metropolis in South Africa. The paper described how a poster creation campaign was used to raise awareness about cyber safety related issues amongst both primary and secondary school children. The paper briefly presented the researcher’s observations during this campaign and some lessons learned which could help contribute towards the success of future campaigns.

## References


[8] SACSAA: South african cyber security academic alliance
Back to basics: Information security education for the youth via gameplay

Rayne Reid\textsuperscript{1} and Johan Van Niekerk\textsuperscript{2}

\textsuperscript{1,2} Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
s208045820@live.nmmu.ac.za, Johan.VanNiekerk@nmmu.ac.za

Abstract. Cyber technology and information resources are both fundamental components of everybody’s daily life. This means that both society’s adults and youths are exposed to both the benefits and dangers that accompany these resources. Cyber security education is becoming a necessary precaution for individuals to learn how to protect themselves against the dangers of the technologies and resources. This is particularly important for the current and future youth who are the most technology literate generations. This paper presents a novel educational approach that can be used to introduce information security concepts to the youth from a very young age.

Keywords: Information security education, Case study, Educational Gameplay, Brain-compatible Education

1 Introduction

The 21st century has witnessed numerous technological innovations and developments. Several of these developments have involved information technology (IT) infrastructure. These information technologies and their companion “cyberspace” have gradually become commonplace in many aspects of modern life. As a result users are becoming increasingly dependent on these technologies and cyberspace.

Unfortunately although cyber space provides many advantages to a user, it is also introduces many dangers to the user. The exposure of people, old and young, to the online and interactive world has resulted in them becoming potential targets for a vast array of information security threats. Examples of potential threats may include online attacks, exposure of personal information and many possible scenarios in terms of which other people pose a threat to the user by their using technological channels to reach an intended victims \cite{1}. It is, thus, essential that individuals learn to protect themselves against these dangers. This is particularly important for the current and future youth who have grown-up in this technology-saturated environment.

The current youth are often more technology literate that the older generations. Generation Y (born 1977-1990) and the online teens (born 1991 – now, including generation Z) account for over 30\% of the internet user population \cite{2}. Similarly Generation Z (born 1995 – 2012, over 23 million people) are often already using the internet and other technologies. Generation Z has grown up in contact with highly sophisticated media and computer environment and will be more Internet savvy and
expert than even Generation Y [3]. This trend has persisted since the start of the development of most modern technologies. It has thus resulted in the question of “How can the youth be educated about cyber security?”

Traditionally children have looked to their parents to teach them how to cope with danger. However in the case of technology-related lessons, parents are often less technology literate or educated than the youth. As a result they are seldomly equipped to teach kids cyber safety. A more creative and semi-/fully-formalized information security education approach is therefore needed.

This paper examines a novel approach, which introduces a brain-compatible information security game. It will focus on the introduction of information security awareness games, which were accompanied by information security awareness talks into a primary school class as a case study environment. The games themselves will be created to comply with the brain-compatible pedagogy.

2 Background

2.1 Information Security Education

Information security is a multifaceted problem and a comprehensive solution to this problem will normally encompass physical, procedural and logical forms of protection against threats [4]. Information security education provides the knowledge and skills needed to implement information security practices.

Traditionally formal information security education programs have mainly targeted organisational audiences. However recent national legislation and cyber awareness campaigns (such as the campaigns run in the UK and USA) target the general public[5, 6]. This implies the inclusion of the youth as well. Cyber security education that is appropriate for organisational environments would be less effective for educating the youth; therefore a more ‘fun’ approach is required.

2.2 Children and educational play

Traditionally formal education approaches have been adopted for information security education; however this may not be an effective approach for a very young target audience. A more fun approach may be more suitable for such an audience. However should a fun approach be adopted, it should still implementable in a formal education environment. This would take advantage of the fun aspect as well as the formal education environments tendency to augment and build upon fundamentals taught using the fun approach. An educational game may therefore be an effective solution.

The young of many species learn skills though gameplay e.g. lion cubs learn to hunt and fight through mock battles and hunts with litter mates and later ‘practice prey’. Similarly young humans learn skills through ‘make believe’ and educational games which enable fun learning.
Admittedly this learning is not completely sufficient for current life; however it is the basic building blocks, which provide the foundation knowledge which may be augmented by formal education. It is therefore the focus of this research for introducing knowledge to the youth.

‘Fun’ Education is an effective mechanism for people, especially of children, as it has the added benefit of holding their attention, being fun, engaging their interest, and preventing the children from disassociating from what is being learnt and done [7]. It does however require structure to be effective as an education toll. This can be accomplished through the introduction of pedagogy to the game, so as to help promote learning. One, tried and tested, pedagogy is brain-compatible education.

2.3 Brain-compatible Education (BCE)

Brain-compatible education may be defined as learning based on the educational principles, methods and techniques which endeavour to teach subject-matter in a manner and format which is naturally complementary to the physical and psychological processing functions of the brain [8, 9].

This means it is an approach that manipulates education presentations and environments to appeal to natural learning processed. To achieve this brain-compatible educators design and orchestrate life-like, enriching, and appropriate experiences for learners [10]. This means that instructional strategies are employed to allow all students may process information more effectively so as to ensure maximum understanding, retention and recall [11].

Brain-compatible principles and techniques have been effectively used in real-world classrooms and some online environments in the presentation of formal lessons. Its implementation is guided by a number of principles some of which are presented in Table 1.

Table 1: Brain-compatible principle applied in the design of the artefact [7]

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A learning experience should be as multifaceted as possible, catering for as many learning styles as possible and providing as many opportunities for each learner to develop as possible</td>
</tr>
<tr>
<td>2</td>
<td>Positive emotions should be used to aid recognition and recall</td>
</tr>
<tr>
<td>3</td>
<td>Relate all new material back to old material and thereby build new knowledge on old knowledge</td>
</tr>
<tr>
<td>4</td>
<td>The search for meaning is innate and occurs through patterning</td>
</tr>
<tr>
<td>5</td>
<td>Every brain simultaneously perceives and creates parts and wholes during the learning process</td>
</tr>
<tr>
<td>6</td>
<td>It is necessary to review material repetitively to solidify recall and recognition</td>
</tr>
<tr>
<td>7</td>
<td>Both the focused and peripheral attention of a learner should be involved in the learning process</td>
</tr>
<tr>
<td>8</td>
<td>Allow learners to progress through the course at their own pace.</td>
</tr>
</tbody>
</table>
These simple and neurologically sound principles are the general theoretical foundation of brain-compatible education [10]. When applied to educational material the brain-compatible principles guide educators in the definition and selection of appropriate educational programmes and methodologies and presentation techniques. Some of these principles will be applied and explained in the creation of the research artefact. The relevant principles are presented in Table 1. The next section will examine the case study portion of this research.

3. Case Study

3.1 Methodology

This research will follow various procedures of the case study protocols described by Yin [12] and Creswell [13]. The structure of the paper will be to firstly provide the context of the case study and its experiment; secondly to describe the research artefact, thirdly to describe the research instrument and fourthly to describe the implementation of the case study experiment. Finally the results and analysis of the research will be presented with accompanying conclusions which have been reached.

3.2 Description of the Context

Cyber security is a topic that is seldomly addressed in current South African school environments. Until recently this has been an acceptable practice. However because cyber technologies and information facilities have integrated into the daily lives of many people, including children of all ages, it has become necessary to educate children about cyber awareness and security. The subject matter should therefore be gradually introduced to the young target audience.

The context in which this case study occurs is at a primary school level (ages 7-13), using educational gameplay as the first subject matter primer. A fun information security game (research artefact) therefore had to be developed. The design of the artefact had to be carefully considered, this is discussed in the next sub-section.

3.3 The Artefact (Creation of BCE Information Security Board Game)

The artefact is targeted at a primary school audience. Therefore considerations in the design of the game included: age appropriateness content and delivery, inductivity or familiarity of use, ease of understanding, level of learnability and the potential for compliance with brain-compatible education principles. Existing children’s games, which targeted this age group, were considered as the basis for the artefacts design.

‘Snakes and Ladders’, a popular board game played by children in many cultures, was chosen as the foundation game on which the information security educational game would be based. Numerous reasons accounted for this decision. Firstly the
game, having existed since the 2nd century in India, is a popular game whose gameplay and rules is probably known to the target audience [14]. Secondly its original purpose of teaching children the difference between 'good and evil' is similar to teaching children good and bad information security behaviours [14]. Thirdly, it currently targets children from age 7+. Fourthly pedagogical principles and appropriate information security educational content could be easily incorporated into the design. The design, content, and game play rules will be discussed in the below sub-sections.

3.3.1 Design

This section will present the reasons why ‘Snakes and Ladders’ was selected as a good redevelopment candidate for this research. These reasons will also be linked to implementation considerations from a brain-compatible educational perspective. The focus of this section is therefore the presentation design.

Firstly the game had to cater for multiple learners learning rates. Brain-compatible education advocates self-paced progression (Principle 8) therefore this had to be catered for in the game environment. This was achieved by presenting the content in a game format which required the players to take turns, and to move according to a dice throw. This therefore allowed the learners to play and learn at their own pace, but ensured that the dice regulated the general pace of the entire the game. In brief it prevented overly long pauses, such as those experienced in games such as chess.

Secondly the design, or redesign of the game had to maintain the interactivity and “fun feel” of the game. This was necessary to ensure a mental and physical involvement in the game, a social and communicative experience, and a fun, peer-supported learning experience. This was considered essential as it implements Principle 1 by appealing multiple learning styles, especially those favoured by kinaesthetic and auditory (social) learners.

Thirdly the game had to be entertaining enough to hold the player’s focused and peripheral attention. This was necessary so as to comply with Principle 7. The abovementioned interactivity and social nature of the game would help achieve this. Interactivity combined with the “fun factor” of the game, the learner would become emotionally stimulated, and this would cause further interest and encourage focus.

The “fun factor” of the game also appeals to the learner’s positive emotions. Principle 2 advocates that a learner is more likely to learn and retain content if they are experiencing positive emotions. Negative emotions may result in distraction, disinterest and the prevention of knowledge retention. Many aspects of gameplay appeal to this principle. Firstly a game, by its nature is fun, with its design encouraging changes in the emotional state e.g. happiness for ascending a ladder. Secondly the interaction between learners enables fun communication and competitiveness. Finally winning as incentive, increases the fun factor and appeals to Principle 2, it also encourages progression throughout the game (Principle 8). This emotional appeal is also further encouraged through the use of colour on the board.

Colour was used to influence the emotional state of the learners and also their focus – Principle 2. The background of the board’s lesson material was coloured
various shades of yellow and green (see figure 1). Yellow, the first colour to be distinguished by the brain, elicits positive moods and attracts the learners’ attention [15]. This change to the material also relates to principle 7 and the enhancement of the learners’ attentiveness. Green encourages productivity and long-term energy and is, thus, an appropriate colour for a classroom activity [15]. The colours used also implemented principle one, by engaging visual learners. This type of learner is particularly drawn to colours, graphics and written concepts. These learners would therefore be the most likely to focus and benefit from the built-in education mechanisms of the “Snakes and Ladders” game.

Figure 1: The Research Artefact - Snakes and Ladders Password Board

The final design considerations relate to the educational reinforcement mechanisms. As an educational tool, the game has to provide consequences and rewards for lessons learned during the game. This was easily introduced into “Snakes and ladders” as its original purpose was to teach the difference between good and evil, and such mechanisms were therefore already inherent.

Information Security lessons/messages was placed above snakes and below ladders on the board (see figure 1). Positive lessons were reinforced by enabling ascension of the board via ladders. Conversely negative lessons were reinforced by forcing the player to descend down the board via snakes. This design associated negative consequence with negative message and positive consequence with positive message, and thereby enabled behaviour patterning (principle 4). This patterning also enabled principle 5 by creating knowledge components around a central topic which the player learned as a whole concept.

The snakes and ladders where placed randomly throughout the board, alongside information security lessons. These designs, and other similar designs, were used to present a number of different topics. The content presented in this case study will be addressed by the next section.
3.3.2 Content

Multiple games were created for many different topics. Examples of topics included social networking, password security, and virus security. Each of the boards had a similar design, but different content. The board presented, which relates to the results reported by this paper, taught password security content.

The content included within the game was topic related, in this case pertaining to secure password management. Various rules specifying the do’s and don’ts of password security were placed above snakes and below ladders (see figure 1).

The do’s and don’ts included lessons such as: the creation of a strong password, the frequency of change required to ensure a secure password, whom the password may possibly be shared with etc. They were written in a format that the player had/had not complied with a ‘rule’ of secure password management. The ‘learner-centric’ perspective serves to conform to Principle 3 of brain compatible education of contextualising lessons from a learner’s viewpoint.

The do’s were placed below the ladders e.g. “Your password is at least 8 characters long”. The don’ts were placed above snakes e.g. “You gave your password to a friend”. A complete list of the lessons presented in this particular password board is presented in Table 2.

<table>
<thead>
<tr>
<th>Do’s</th>
<th>Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td>You gave your password to your parent or guardian</td>
<td>You gave your password to a friend</td>
</tr>
<tr>
<td>Your password is at least 8 characters long</td>
<td>Your password is less than 5 characters</td>
</tr>
<tr>
<td>You change your password at least once a month</td>
<td>You wrote your password down</td>
</tr>
<tr>
<td>Your password is not a word in the dictionary</td>
<td>You used your name or your pets name as a password</td>
</tr>
<tr>
<td>You used characters like !,#,$ in your password</td>
<td>You used the same password everywhere</td>
</tr>
<tr>
<td></td>
<td>Your password is easy to guess</td>
</tr>
</tbody>
</table>

These lessons were then learnt in accordance with the rule of the ‘Snakes and Ladders’ gameplay. These rules will be presented in the next section.

3.3.3 The Rules of play

The ‘Snakes and Ladders’ games can be played by 2-6 players. Each player has a token which the place and move on the board. Play begins with everyone’s token being placed at the start of the game. The first player then rolls the dice and moves the token along the sequential squares according to the number thrown.

If the square a player lands on contains an information security educational message, they read it out loud and perform the accompanying action. The verbal sharing of the message helps the learners to cognitively consider the lesson (principle 1). If the message was a do not lesson, they are swallowed by the snake and move
their token to the square which contains the snake's tail. If the lesson was a do they ascend the ladder and place their token in the square at the top of the ladder.

Players take sequential turns to roll the dice and move their tokens. The first player to reach the 50th square (Finish) is the winner.

The effectiveness of this research artefact as an information security educational tool will be determined through a survey. The survey (research instrument) used to do this will be presented in the next section.

3.4 Research Instrument

Part one of the research instrument consisted of a survey designed to acquire quantitative data about whether the learners had gained knowledge about secure password management after playing the game. The questions on the survey dealt with the subject area on which the game focussed. They were close-ended, multiple choice questions which related to a few select lessons that were included on the board. These tested student knowledge gain.

Part two of the research instrument consisted of a few interview questions targeted at teachers who allowed their classes to play the game. The interview questions tried to determine the teacher’s perceptions of the effectiveness of the game as a teaching tool and it’s the perceived effect on the learner’s knowledge and behaviour.

Both parts of this research instrument were implemented alongside the research artefact in the context of the case study. This is presented by the next section.

3.5 Implementation (experiment)

The research artefact was freely distributed to many primary schools within South Africa. Some of the schools targeted in the distribution were also given an introductory information security awareness talk and lesson using the research artefact. However for the purposes of this case study, two schools were selected as a target group and their data was gathered.

At School-A a grade 5 class of eleven students between the ages of eleven and twelve participated. At School-B a grade 3 classes of fifteen students between the ages of nine and ten participated. Both class teachers ran the survey in their classes, and then were themselves interviewed by the researcher. The research was conducted in this manner to comply with ethical research policies.

In relation to ethical research, children are classified as a vulnerable target group. Therefore due to ethical considerations both internal at Nelson Mandela Metropolitan University (NMMU) and externally at the target schools, the researcher did not interact directly with the students.

Surveys were provided to the target school’s teachers. The teachers first had the children answer the surveys before playing the game. After the answer session, the children were then asked to play the game. After the game had been played they answered the survey questions a second time. The children were not allowed to share or discuss their answers. The researchers later interviewed the teachers.
This implementation was used as this research is the first stage of a larger research goal. The results presented are relevant to each case, however due to a lack of double blind testing they are not formal enough for statistical significance. A statistically significant approach will be conducted in the next stage of this research.

3.6 Results and Analysis

Within the survey, three questions, which related to the lessons presented in the game, were asked. These questions were asked before and after the game activity to determine whether there had been a change in the learner’s knowledge and response. The results showed a definite positive trend which confirmed that the learners had gained knowledge relevant to secure password management (see Table 3).

Table 3: Aggregated Learner Survey Results

<table>
<thead>
<tr>
<th>Question Number</th>
<th>Before playing the Game</th>
<th>After playing the Game</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Correctly Answered (%)</td>
<td>Incorrectly Answered (%)</td>
</tr>
<tr>
<td>1</td>
<td>53.33</td>
<td>46.67</td>
</tr>
<tr>
<td>2</td>
<td>34.62</td>
<td>65.38</td>
</tr>
<tr>
<td>3</td>
<td>66.67</td>
<td>33.3</td>
</tr>
</tbody>
</table>

The interview questions aimed to determine: whether the teachers perceived the game as an effective teaching tool; and whether they perceived the learners to be more aware of the matters which the game taught after the game had been played.

Both of the teachers felt that the learners had definitely learned valuable lessons, relating to the topic, via the game. They also observed that the learners had undergone small behaviour changes which indicated a higher awareness of the issues. Both of the teachers concluded that they perceived the ‘Secure Password – Snakes and Ladders’ game to be an effective education tool.

4. Conclusions

Information security education is necessary for today’s youth. Gameplay is an effective knowledge delivery system for youth, and can be used as a delivery mechanism for information security educational lessons. Such education does not have to be in an online environment. This case study has shown how a traditional board game approach could be effectively used in classrooms for such education. The case study has shown that the playing of this game lead to information security knowledge gain and to a certain amount of retention amongst the case study’s students. It is therefore the conclusion of this author that gameplay in this format could be a viable option for the education of the future generation. Further research should be done to further improve the process.
5. Future Work
The research shown in this paper forms the preliminary starting stage of a larger information security education research plan. The next stage will prove effectiveness via controlled studies in order to prove statistical significance.

6. Acknowledgement
Professor R.Von Solms is acknowledged for his game content contribution.

7. References
Towards a Brain-Compatible Approach for Web-Based, Information Security Education

R Reid and JF Van Niekerk

Institute for ICT Advancement, Port Elizabeth, South Africa
e-mail: S208045820@live.nmmu.ac.za; Johan.vanniekerk@nmmu.ac.za

Abstract

Information Security is becoming a necessity for all information users. Suitable delivery and presentation of information security education to these users is therefore becoming increasingly important. Online learning may be a suitable mechanism. It has become a widely used, extensive education format that uses information and communication technology as well as the many resources available on the web. In order to ensure an effective and enjoyable learning experience online education should emulate real-world ‘classroom education’ and be designed in compliance with pedagogy. Brain-compatible education (BCE) is such a pedagogy. BCE has primarily been used in real-world classrooms. This paper examines how generic, online, information security education can be developed in compliance with BCE principles in the Moodle environment.

Keywords

Information Security Education, Brain-compatible Education, E-learning, Moodle, Case study

1. Introduction

Information security education had long been an acknowledged need in an organisational context (NIST 800-16 1998). However due to recent changes in and the creation of new national legislation and cyber security initiatives, this need has now been assigned to the organisation and the general public. The educational target audience therefore includes individuals from all age groups, education levels and social standings. The current generation would be the most affected by this change.

The current generation of learners has grown up in a media-rich environment. This environment has predisposed them to prefer information presented in an entertaining and interactive manner. Consequently, this generation will be the first capable of benefiting from the educational aspects of the web and interactive web technologies.

Educational approaches which use computer network technologies, primarily over an intranet or the Internet, to deliver information and instruction to individuals are fast becoming a popular education method (Welsh et al. 2003). It has many advantages such as easy accessibility, target audience diversity and development versatility. Unfortunately web-based learning courses often mirror real classrooms. Therefore in many educational fields including information security, the problems that exist in real classrooms also exist in web-based learning environments.
Educational researchers are continuously searching for pedagogies that can improve the learning experience in any real classroom. Many of these pedagogies could potentially also be applied in online environments. Brain-compatible education (BCE) is one such pedagogy that has been successfully used in real classrooms.

Brain-compatible education is designed to take advantage of the relationship between an educational environment and the natural complexities of the human brain (Jensen 2008). Several BCE principles, methods and techniques have thus developed. These techniques endeavour to teach subject matter in a manner and format which is naturally complimentary to the brain’s physical and psychological processing functions (R. N. Caine & G. Caine 1991). BCE’s application to the design of online learning environments has been proposed by Clemons (2005), this paper will apply and test it on an online information security course.

This paper aims to show that BCE principles can be applied in the Moodle 2.0 environment when developing an information security course to be appealing and effective for a learner’s information security education experience. The methodology which was used is presented in the next section.

2. Methodology

This paper takes the form and structure of a case study, as described by Creswell (2007). The structure is as follows: an entry vignette, introduction, description of the case and its context, development of issues, detail about the selected issues, assertions, and closing vignette.

The research itself was conducted as a case study wherein material from an existing information security course was selected and modified to comply with BCE principles in the Moodle environment. Some of the changes made where previously theorised possible by Reid, Van Niekerk and Von Solms (2011). This paper focuses on the lessons learned during the actual implementation of the design guidelines which could be applicable in future online, BCE cyber security courses.

3. Context of Case study

SEAT was the course selected for modification during the case study. SEAT is a security education and training course at the Nelson Mandela Metropolitan University (NMMU) which targets students and the general public. Its objectives are: to improve awareness of the need to protect system resources and an organizations end users; to develop the skills and knowledge of computer users so they may securely perform their computer activities; to allow online access to a rich source of security related best practices; to help end users understand why security is part of their responsibilities, and how they impact their organizational employers security.

The original SEAT consisted of nine modules. Each module consisted of a single flash lesson and a related multiple choice quiz. The lessons content presentation consisted of text and related clipart images. An evaluation of the original SEAT showed that it lacked usability, which necessitated the redevelopment of the course.
Two major additional considerations during redevelopment included the need for it to be as appealing and easily accessible as possible for a diverse, dispersed target audience. Thus it was decided that the course would be modified to be presented in a BCE compliant manner, and made accessible as an e-learning course via Moodle.

4. Case study Background

This section will provide a brief background to the primary fields of study which influenced the choices in the redesign of SEAT as presented later in this paper.

4.1. Online Learning

Many communications, collaboration and education enabling technologies have developed alongside the Internet, computer-based multimedia, and the World Wide Web. These technologies have become an enabler of a new variety of e-learning called “web-based” or “online” learning (Zhang 2003).

Online education has delivered many benefits to education experiences including: improved quality of the learning, improved accessibility to education and training, improved cost-effectiveness of education (Alexander 2001), promotion lifelong learning, enhancement of an educators ability to address different audiences and diversify their teaching style, and use of innovative teaching methods in order to maintain students’ interest (Bates 2001).

Educators have focused on extending traditional learning method and techniques through electronic and web technologies into new dynamic education models and environments (Eckert et al. 1997). Many web-based learning environments complete with material have already been successfully created using a variety of tools. Selecting such a tool was the first consideration.

Many popular, open-source and proprietary learning system tools such as Blackboard, Sakai, aTutor, Schoology and many others exist. Moodle is one such environment which is used at Nelson Mandela Metropolitan University (NMMU). Therefore, due to convenience and availability of this platform, it was chosen for the case study. However the similarities which exist between the various online learning management systems and their supporting web-technologies, may mean that this case studies assertions may be applicable to other platforms. The next consideration was engaging the learners.

The aim of any educational experience is to ensure learners accept, retain, and process information which is presented to them during a learning experience. To fulfil this goal the learners should be interested, engaged and motivated to participate in the learning experience. Learning principles and conditions should therefore be used to present material in a manner which meets learner needs (Clemons 2005). The application of pedagogy to e-learning courses is therefore recommended.
4.2. Brain-compatible Education

Brain-compatible education (BCE) is defined as learning based on principles, methods and techniques which endeavour to teach content in a manner and format which is naturally complimentary to the brains physical and psychological processing function for incorporating information into its schema (Jensen 2005).

Brain-based education involves teaching through the designing and orchestrating life-like, enriching, and appropriate experiences for learners (R. N. Caine & G. Caine 1991). It is a pedagogy which addresses multiple modes of learning, acknowledge outlets for creative presentation of learning, provide enough contrast to preclude boredom, and contribute to a motivating context (Rogers & Renard 1999). It accomplishes this by using effective teaching methods, techniques and approaches from all educational disciplines to enhance subject matter to be as appealing and learnable as possible for the brains of the target students (Jensen 2008).

Target audiences for classroom-based BCE learners have ranged from primary school to university students. The application of this pedagogy has been proven to positively affect students’ learning (Jensen 2005). Clemons (2005) suggested the application of the pedagogy to online, but did not provide any technical details on how this could be done. This paper aims to explain how the pedagogy can be implemented in a Moodle context for an information security course.

4.3. Moodle

“Moodle is an Open Source Course Management System (CMS), also known as a Learning Management System (LMS) or a Virtual Learning Environment (VLE)” developed in compliance with a "social constructionist pedagogy" (Moodle.org 2012). It is a tool used by educators to create dynamic, online websites for the delivery of their course to their students.

Moodle courses consist of an educator’s chosen activities and resources. An activity is something that a student will do that interacts with other students and or the teacher (Moodle.org 2012). There are thirteen standard Moodle some examples being assignments, forums, wikis, quizzes and lessons (Moodle.org 2012). A resource is an item that an educator can use to support learning (Moodle.org 2012). Standard resources included by Moodle are files, folders, IMS content packages, labels, HTML pages and URLs. All courses can be augmented through the use of plug-ins.

Moodle can be used to conduct entirely online courses or it can be used as an augmentation tool for their interpersonal classes (Moodle.org 2012). NNMU has mainly used it as an augmenter tool; however with the creation of SEAT it is also being used as the sole material provider for an entirely online effort.

For the purposes of the case study presented in this paper, Moodle was the chosen LMS for the implementation of a BCE compatible version of SEAT. The next section will identify the issues which were addressed in the case study.
5. Identification of Issues

This section will briefly outline a few issues addressed by the redevelopment of the SEAT course. The problems are separated into two categories: Learner-related and Educational-Material Related.

5.1. Learner-Material Issues

Many issues/factors required addressing so as to improve the learners education experience. The first issue is that the target audience is the general public. Therefore the material has to cater for a large variety of learning style preferences. Furthermore because the audience is so varied in age, abilities, background and culture etc. the material had to be as appealing as possible to as many people as possible.

The second issue is that in traditional, ‘compulsory learning’ schools or organisations are able to “force” the completion of an activity or course through cohesion of various forms; in a voluntary online education scenario this cannot be replicated. Therefore alternative measures must be used to motivate a learner to learn. Thirdly the existing SEAT material encouraged learning by rote. This an issue because remembering material by rote is the lowest level of Blooms taxonomy of the cognitive domains (Van Niekerk 2010). Cyber Security Education learners need to understand the material so as to be able to apply it.

The fourth issue is that the current standard material is presented in a non-explanatory manner. As a result of this presentation style, the learners are often distracted by other activities. The fifth issue is that the modules are currently presented as isolated segments of the course with no tie into the overall concept of what is being taught. The context in which the material is taught is also not always relevant for a student. Finally in the original material no feedback was provided to the learners. This is problematic, as formative feedback is necessary in any education approach. This concludes the learner –material issues, the next section will identify the material-creation issues.

5.2. Material-Creation Issues

In addition to the learner related factors; discussed above; factors such as how the material is developed, hosted and accessed also needed to be addressed. Firstly the original application was difficult to maintain. This is because code maintenance, over a number of years, was poorly documented. This is further aggravated by the fact that the development language and development environment used to create the original SEAT is outdated and no longer functions well on current computers. Thirdly the material was not very accessible. Learners required access to an installation of a desktop application, this limited a learner’s ability to access the material to traditional class and lab time. Finally there was no automated control over who could enrol in the course and therefore the course “graduate” was tracked manually. Therefore this system was vulnerable to human error.
The issues identified in each category will each be elaborated upon in the next section. The solutions applied in the redevelopment of the material will be provided.

6. Detail of selected Issues

This section elaborates upon the previously discussed issues which will be further explained and related to the brain-compatible pedagogical principles. For additional brain-compatible principle explanations refer to Reid et al. (2011). The brain-compatible principles which will be addressed are listed in Table 1. Each principle has been assigned a non-meaningful number which, for the sake of convenience, will be used for all further references to the same principle within the paper.

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A learning experience should be as multifaceted as possible; catering for many learning styles and providing as many opportunities for each learner to develop as possible.</td>
</tr>
<tr>
<td>2</td>
<td>Positive emotions should be used to aid recognition and recall.</td>
</tr>
<tr>
<td>3</td>
<td>It is necessary to repetitively review material to solidify recall and recognition.</td>
</tr>
<tr>
<td>4</td>
<td>Both focused and peripheral attention of a learner should be involved in the learning process.</td>
</tr>
<tr>
<td>5</td>
<td>Every brain simultaneously perceives and creates parts and wholes during the learning process.</td>
</tr>
<tr>
<td>6</td>
<td>Relate all new material back to old material and thereby build new knowledge on old knowledge.</td>
</tr>
<tr>
<td>7</td>
<td>Allow learners to progress through the course at their own pace.</td>
</tr>
</tbody>
</table>

Table 2: Brain-compatible education principles

The original material of the SEAT course was moved to the Moodle environment. Once it had migrated the authors began the process of updating the material and course to solve the various issues. The redevelopment of the course will now be explained.

6.1. Learner-Material Issues

Firstly it was determined that to implement Principle 5 learners had to understand how material exiting as an isolated concept and as a part of an overall cyber security approach. To do this Moodle’s ability to separate course material into modules and blocks was used. Each lesson from the seat course was assigned to a module. Within each module a lesson activity, a quiz and additional resources were included.

Modules were structured in a progressive sequence. Initially only the first module was accessible. To progress through the course the learners had to achieve a minimum required mark in each modules quiz. This progressive design was it ensured the material was viewed in a particular order. This aided principles 5 and 6. The content could relate material back to the previous modules material, ensured that learners had the required “old” knowledge and provided perspective as to how the concept fitted into the whole subject.
Within the module itself the learners were free to navigate through the lesson material and the additional resources according to their own preferences. The grouping of the activities and resources complied with Clemons’ (2005) suggestion of “chunking” activities together to help them relate and make sense. By allowing learners to review the modules material in any particular order they were allowed to progress as a self-determined pace. This combined with the allowance for the active modules quiz to be completed at any time promotes Principle 7.

Schools or organisations can insure the completion of traditional compulsory learning activities through cohesion of various forms. In a voluntary online education scenario this cannot be replicated. Therefore alternative measures must be used to motivate a learner to learn. Learning requires motivation and engagement this is particularly important since online learning is a self-managed endeavour.

The next aspect of the redevelopment dealt with the redevelopment of the material itself. This redevelopment had to aid compliance with the Brain-compatible principles 1, 2, 3, 4 and 6.

Initially, the Moodle lesson activity was considered for the SEAT lessons. Moodle lessons allow navigation between question pages and content pages, and it has adaptive ability to navigate between pages based on the learner’s response. However because the lessons consist of basic HTML it was determined that they were not dynamic enough for our needs. Instead, Microsoft’s Sketchflow Silverlight application was used to create lessons which were then hosted on a server as a webpage. This webpage was then embedded in the Moodle module as a URL resource. The aim was to create interactive, media-rich and engaging lesson material.

The Moodle course targets the general public. This means that the learner audience consisted of individuals who varied their age group, culture, experiences, abilities and learning-style preferences. The course material had to appeal to as many of these individuals as possible to ensure successful learning experience. To enable the brain-compatible principles 1 and 2 were applied to the redevelopment of the material.

Clemons (2005) suggested the inclusion of “elaborate rehearsal” and interactivity in an online course to aid compliance with these principles. Activities which Clemons theorised complied with her suggestions were audio-, video- and animation clips, role plays, debates, voice-overs lectures, use of colour, diagrams, charts, pictures, interactive models and drawing activities.

In the redeveloped SEAT we included video clips, music, and lesson materials containing text, contextual pictures and clarifying animations. Colour was used to influence the learner’s emotional state.

The background of the lesson material was styled yellow; this elicits positive moods and aimed to attract the learner’s attention. This aspect of the material also related to Principle 4 and the enhancement of the; learners attention. Future modifications of the material will incorporate green into the colour scheme as it encourages productivity and long-term energy are good in classrooms (Taylor 2007). Because of
NMMU policy, the Moodle environment itself was styled to conform to the NMMU, colour branding which is not necessarily brain-compatible. This will be tested in future research.

Clemons (2005) suggested that interaction would enhance attentiveness in online courses. The use of techniques to stimulate emotions such as excitement, fun, curiosity and anticipation to enhance learning (Clemons 2005). All this aids compliance with principles 1, 2, 3 and 5. Role-playing and scenario simulations and thought provoking games, videos and animations were suggested by Clemons as suitable techniques. Unfortunately role-playing and scenario simulations are currently only planned features of Moodle (Moodle.org 2012). To resolve this issue we included video resources and animations which illustrated the concepts in an interactive manner in the material. These additions also aimed to focus the learner’s attention on the material and prevent distractions (principle 4).

Principle 3 was reinforced multiple time since the material was provided in many formats and included many elements which repeated the concepts in different contexts while appealing to principle 1 by catering for all learning styles.

Finally the courses and its quizzes and exams were modified to provide formative feedback. This modification complied with Clemons (2005) suggestion of providing encouraging, positive feedback and avoid penalizing mistakes that come from the learning curve associated with technology.

6.2. Material-Creation Issues

There are many ways the brain-compatible principles can be applied in the Moodle environment. The applications used in this case study to aid the learners in their interaction with course material are only a few examples of this. The next section will address how the issues relating to the materials creation and hosting were dealt with.

The Technology Acceptance Model (TAM) indicates that when users are presented with a new technology the perceived usefulness and ease-of-use will influence their decision about how and when they will use it (Venkatesh & Davis 2000).

Since the online material was designed for Moodle, the material had to be hosted on a Moodle server. NMMU has an internal campus-wide Moodle server. The use of Moodle addressed most of the issues in this category.

The issue of accessibility was partially solved because Moodle can be accessed online. Learners are able to access their Learn sites anywhere at any time. However currently the NMMU Moodle server only allows registered NMMU students to log in and register for courses. Internal policies have issued a practice of disabling manual registration procedures. Therefore a lecturer cannot register a student who is not physically studying at NMMU. This issue will be addressed by moving the SEAT course to an external server.
The material is now maintainable as the Moodle platform is constantly be updated by its developers and all the changes are well documented. The actual lesson material used in the SEAT case study is also updateable and editable via Microsoft tools e.g. Expression blend and Visual Studio 2010. All Microsoft projects are backwards compatible.

Moodle’s multitude of features are very useful in the creation and design of an education experience. However the default, online creation methods of various activities are not always ideal, and can be tedious or time consuming e.g. the quiz development feature. The native Moodle quiz interface was time consuming and not ideal for the development of many questions simultaneously. We used a third-party tool called Respondus as an alternative.

7. Assertions/Lesson Learned

Firstly based on a preliminary evaluation of the learner’s reactions to the redeveloped material we have found the following: 100% of the learners liked the look and feel of the material; 85% of the learners like the variety of educational material provided; and 80% of the learners felt motivated and engaged during the learning experience.

Secondly the authors wish to assert that based on the case study’s course redevelopment and subsequent launch that it is possible to create brain-compatible, online information security material. Furthermore it has been well demonstrated that Moodle enables the development of brain-compatible information material even though it is created to enable a different pedagogy. It should however be noted that the creation process is not always easy, and the built-in development tools are not always very usable or suitable for mass development. The authors recommend the employment of third-party tools when necessary.

Finally, it is the opinion of the authors that there is a requirement for the development of tools which cater specifically for information security educators who wish to create brain-compatible education material.

8. Conclusion

Moodle is an education platform which can be used in compliance with BCE principles to create online, information security. However some of its creation features are not as comprehensive or usable as they could be. In these cases the use of third-party party tools is recommended. To further enable information security educators to create online, brain-compatible, information security education material, both using and independent of Moodle, a layer of applications and tools which cater specifically for the needs of material creating educators needs to be developed.

9. References


Information Security Culture: A General Living Systems Theory Perspective

Rayne Reid
School of ICT
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
s208045820@live.nmmu.ac.za

Johan Van Niekerk
School of ICT
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Johan.VanNiekerk@nmmu.ac.za

Karen Renaud
Computing Science
University of Glasgow
Glasgow, Scotland
Karen.Renaud@glasgow.ac.uk

Abstract—Information security culture (ISC) is often acknowledged as being a vital subculture within an organizational culture. As a subculture, its purpose is to fulfill its security purpose, while integrating into, and supporting, the broader organizational culture. However, in contrast, few discussions of ISCs acknowledge that the ISC itself is comprised of subcultures. The research literature’s lack of exploration of this nested nature of ISC may be hindering in-depth understanding of the ISC as a system within itself, as well as within the broader organizational culture. This paper will therefore address this by straying from traditional views of ISCs. We will examine an ISC as a self-managing, self-repairing collective of multiple ISCs which meet the organizational culture’s security needs. The paper’s objective is to show that an ISC can be viewed and understood as a living system.

Keywords—information security culture; general living systems theory, conceptual

I. INTRODUCTION

Many organisations acknowledge that the creation of an acceptably effective information security solution is of vital importance [1]. Information security aims at securing the acceptable effective information solution is of vital importance. However, in contrast, few discussions of ISCs acknowledge that the ISC itself is comprised of subcultures. The research literature’s lack of exploration of this nested nature of ISC may be hindering in-depth understanding of the ISC as a system within itself, as well as within the broader organizational culture. This paper will therefore address this by straying from traditional views of ISCs. We will examine an ISC as a self-managing, self-repairing collective of multiple ISCs which meet the organizational culture’s security needs. The paper’s objective is to show that an ISC can be viewed and understood as a living system.

Employee actions and behavior are particularly important in an information security solution, as almost all information security solutions rely, to a certain extent, on the humans involved in the security process making the right decisions and acting securely [3]. While technology and processes can be formulated so as to be theoretically secure, the true level of security of such technology and processes relies on the people involved in their use and implementation [4]. The extent to which people use technology securely and comply with the mandated secure processes can drastically affect how truly secure these components are.

People can both consciously and unconsciously become a threat to any information security solution [5]. When they become a conscious threat it may be with a specific intent or because of negligence. Alternatively, when they become an unconscious threat it may be for a range of reasons, including a lack of knowledge of security practices, an inability to properly apply their knowledge to their own work role or environmental context, because they have been conned or due to common negligence. Regrettably, as a result of this it is more likely that a breach that occurs in an information security solution is the fault of humans, and not technology [3]. This threat has become known as the “human factor” in information security.

The establishment of an organizational information security culture (ISC) has been widely accepted as the appropriate counter to this “human factor” threat [4]. The theory supporting this solution being that the creation of a security-conscious corporate culture could potentially lead to employees adopting secure, work-related behavior as a behavioral default [1], [5].

An ISC is often acknowledged as being a subculture of the larger organizational culture [1]. However, it is rarely acknowledged that it can have subcultures of its own. ISCs are, typically, presented in literature as single-level conceptual constructs which are uniformly applicable to all aspects of an organization. However, this representation may be too simplistic to explain the interactions between the interconnected secure business activities and the components of a comprehensive organizational ISC. Therefore it may be advantageous to examine an alternative view if ISC.

An ISC could be viewed as a collection of nested systems that display emergent properties and are also self-maintaining and self-repairing. These properties match the primary characteristics of general living systems. This paper will thus examine an ISC to determine whether it may be viewed as a living system.

Living systems are open, complex, adaptive, self-organizing living entities that interact with their environment or other systems [6]. A living systems perspective will not simplify how we view ISCs. In fact, it will likely complicate it. However, it is our belief that this alternative view of an ISC will reveal considerations of the culture that previous models have failed to identify. This new perspective may therefore assist in developing a further understanding of the underlying components, operations and impact of an ISC. It may enable us to better understand and predict the overall culture and how the organizational and security cultures interact. This, in turn, may affect our understanding of how good ISCs ought to be nurtured and encouraged.

The paper will begin by briefly discussing the concept of ISC; then it will provide a brief overview of general living systems theory and, finally, it will present the way in which an

The financial assistance of the Vodacom/NMMU and National Research Foundation (NRF) scholarships in this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the authors and are not necessarily to be attributed to the sponsors.
ISC could be viewed as a general living system by mapping culture to the system characteristics.

II. INFORMATION SECURITY CULTURE (ISC)

Culture is broadly considered to be the overall, taken-for-granted assumptions that a group has learnt throughout history [7]. ISCs build on this premise.

Many current authors deal with the topic of an information security culture ((8)[9][10],[11], [12],[13], [14]). Most of these authors focus on cultivating, assessing or auditing a culture. To achieve this the authors commonly base their views’ understanding and representation of an ISC on adaptations of Schein’s three-tier organizational culture model [1]. The tiers in Schein’s model consist of underlying assumptions, espoused values and artifacts [7]. However, the model deals with organizational culture in general, not ISC specifically, and the authors cited here seldom provide in-depth explanations about how their interpretation of the adapted model translate to the context of information security. This has left much about the practice to be subjectively interpreted. Van Niekerk and Von Solms have bridged this gap in knowledge by presenting a conceptual model of an ISC and have focused on explaining how its underlying components and processes could influence one another [4]. As a result of the comprehensiveness of the definition, the focus on the conceptualization of an ISC, and the degree of relativity of the explanation of the interactions to the purpose of the research, this paper will adopt their definition of an ISC.

Van Niekerk and Von Solms’s definition of an ISC derives from, and expands on, Schein’s organizational culture model. Schein lists artefacts, espoused values and knowledge as dimensions of his culture model [7]. Van Niekerk and Von Solms expanded the ISC model by concretely integrating the requisite underlying information security knowledge as a separate component in their model [7]. This knowledge dimension was included as the authors theorized that in order to successfully foster an ISC (as a sub-culture within an organizational culture), all business activities would need to be performed in a secure way [12]. Adequate information security knowledge and skills were therefore deemed essential to enable an employee to be able to perform any business activity in a secure manner [4]. According to their conceptualization, an ISC thus consists of four information security related components, namely, artefacts, espoused values, shared tacit assumptions and knowledge [4].

The exact contents of each of the other dimensions were also slightly altered in order to be more context specific to ISC. The ISC-specific interpretation of the model dimensions therefore now refers to the following framework components:

1. Artefacts (AF) – Detailed procedure of the organization’s daily tasks. This dimension includes the visible structures and processes which are deemed to be “measurable but hard to decipher” [4].
2. Espoused Values (EV) – The guidelines for what to include in a policy, and the subsequent ISC, in order to adequately address the business’s needs. These include information security strategies, goals and philosophies.
3. Knowledge (KN) – The necessary and required levels of information security specific knowledge needed to perform the daily business tasks in a secure manner [4].

Within this framework, Van Niekerk and Von Solms explain how these components of an ISC can affect one another [4]. It is necessary to understand these interactions in order to be able to able to predict the strength, stability and predictability of an ISC. Figure 1 illustrates an example.

![Figure 1: Comparison of a stable, secure culture and an unstable, unsecured culture](image)

In brief, the information security-related espoused justifications and official viewpoints [4].

A. Stable and secure B. Insecure and unstable

Figure 1 shows the interactions of an organization’s ISC components and their effect on the strength of that particular ISC. The line labelled BL represents this case’s minimum acceptable security baseline (BL). The side on the left of BL indicates a culture and a set of artefacts that are less secure than the desired minimum BL. The opposite is applicable to the right side of BL. The EV, SA and KN culture components can fall on either side of the baseline. The closer the components are aligned, the more stable the culture is. The consistency of the component strengths determines the strength of the culture. Figure 1 part A shows a culture with well-aligned, strong components. Consequently, the net security level line (SL) of the culture indicates that the combined net effect of all four culture levels is stable and secure. In comparison Figure 1 part B shows a culture with strong EV, a lack of suitable KN, and a lack of the preferred SA. This results in the AF being measured as unsecured. The resultant internal opposition of the culture components results in the culture’s net effect being unsecured and unstable.

This basic explanation of an ISC framework and its components enables us to comprehend the overall conceptual construct of the high-level ISC within the organizational culture. However, this view may be overly simplistic.

We argue that an ISC exists at many levels and in many forms within an organization. It is the detailed ISC components, context and data within each of these individual
and collective subcultures that actually reflect the organization’s true ISC strength and effectiveness. Consequently, the sole use of an aggregated view of an ISC cannot reveal the true, subtle levels of innateness, integration and strength in an organization’s ISC.

An ISC is only as strong as its weakest link. For example, having an aggregated strong password security culture is meaningless if the password security culture in a high-risk department is weak. In such a context it is possible that, as a subculture, the department’s weak password culture could influence the culture of the entire organization. This example demonstrates how different contexts and levels of security can affect the overall ISC. Schein acknowledged the importance of context for an organizational culture. This acknowledgement is also valid for an ISC (as a subcomponent of an organizational culture) and its subcultures.

Schein noted that organizational culture is typically stable and resistant to change [7]. This is partly because culture is the net result of many underlying factors. These same factors will also influence the way culture propagates. Therefore, in order to understand how culture propagates through an organization, one has to understand its context and relationships. This is also true for subcultures such as an ISC. Therefore, there is a need for a view or perspective that acknowledges this interconnection and interdependent nature of an organization’s culture and ISC and the components of the ISC. This is particularly important in order for us to understand how the interconnected nature of the organization’s culture and the SC component, and their various contexts, allow for and affect the development, propagation, maintenance, condition and emergent properties of all the cultures. Essentially, these cultures need to be viewed as self-maintaining and self-propagating systems. A theory which may be appropriate for modelling such a view is general living systems (GLS) theory.

To determine whether this view is possible, this paper will briefly examine a GLS and its characteristics. It will then determine whether the main characteristics of the GLS align with that of an ISC.

III. GENERAL LIVING SYSTEMS THEORY

GLS is a systems theory presented by James Grier Miller in his 1978 book Living Systems. The theory addresses a specific subset of systems, namely, living systems. Miller explores how phenomena occur by examining the relationships a system (organism) has with its environment (possibly a larger organism or system.)

A GLS is defined as being an open, complex, adaptive, self-organizing living system consisting of subsystems that interact with their environment or other systems by processing specific inputs, throughputs and outputs of various forms of matter energy and information [6], [15]. Each of these systems and subsystems can therefore be characterized as purposeful [6].

All living systems comply with the propositions of this definition, whether composite living systems (system of systems) or living subsystems.

A living system consists of many similar components (molecules or subsystems) which evolve and combine to make a larger, increasingly complex, supra-system. Miller proposed that living systems could be divided into eight hierarchical levels, namely, cells, organisms, groups, organizations, communities, societies and supranational systems [15]. Each level increases in complexity and is considered higher than its predecessors as it is a compilation of its lower systems. Each composite system is therefore a suprasystem. Each level and system has its own typical structure and processes which serve the purposes of its own and its hosting environment (or system).

A GLS is therefore typically considered to be a complex entity. It is a system of systems. Each of these systems has a purpose, a process for fulfilling this purpose and a relationship with its environment which helps it fulfill its purpose while receiving from it what is needed by another system to fulfill its purpose.

The detailed explanation of exactly how all of this happens and how a GLS exists and lives is beyond the scope of this paper. Instead, this paper will examine whether ISC can be represented as a GLS when comparing it to some of the primary characteristics of a living system (as described by Miller). These characteristics will therefore be briefly explained and then mapped to an ISC in the next subsection.

IV. MAPPING INFORMATION SECURITY CULTURE TO THE MAIN CHARACTERISTICS OF A GENERAL LIVING SYSTEM

Miller identified a number of key characteristics for a living system. This section will briefly outline five of these primary characteristics.

A. General living systems follow a charter

Miller states that GLSs either contain genetic material composed of deoxyribonucleic acid (DNA), presumably descended from some primordial DNA common to all life, or have a charter [15]. In the case of an information security the latter would be the case.

A charter is the equivalent of a template, original "blueprint" or "program", which guides the creation of the living system’s structure and process from the moment of its origin. Essentially, it is the general plan for the system’s development and operation.

The charter describes the overall system’s purpose and how the system will fulfill this purpose. In terms of an ISC, the authors would like to propose that the primary components of an ISC, namely, the espoused values (EV), artefacts (AF), shared tacit assumptions (SA) and knowledge (KN), map directly to this GLS characteristic.

The ISC components act as a guideline for the structuring of any ISC to fulfill a particular purpose. This is true for high/abstracted levels within an ISC as well as more detail-intensive levels. Basically, they provide the system boundaries and structure. The overall ISC culture has a specific purpose and plan of function and these are the original abstracted ISC components. Derived from this plan, any ISC and its subcultures follow the abstracted charter’s (components) directives while implementing its solution/contribution to the
charter’s fulfilment in a manner which is context-specific to the implementation requirements of its environment.

The plan within the charter (the ISC components) includes guidelines for the creation, implementation, maintenance and possibly governance of the system. Essentially, it guides the system’s development and growth and acts as a baseline according to which these design and implementation decisions may be measured. As a result of this role, the ISC charter and the abstracted ISC components may be considered to be both the system’s charter and the “decider” subsystem in a living ISC.

B. General living systems have a decider subsystem

Within a living system there are a number of critical subsystems which were identified by Miller. Twenty of these essential systems were identified. Owing to limited space, this paper will only focus on the decider subsystem, which in the authors’ opinion is the most relevant. The remaining subsystems, and how they map to the ISC, will be addressed by future work.

In a GLS there exists a “decider” subsystem. This is an essential, critical subsystem that controls the entire system, causing its subsystems and components to interact. It is necessary because without it there would be no interaction and with no interaction under decider control there is no system.

In the context of an ISC, the decider is the decision-making ability needed to initiate and manage the creation, maintenance or change of an ISC. This decision-making ability is representative of the underlying culture change processes which provide the decider with the facts (knowledge) needed to make effective and efficient decisions. This is therefore the representative of the decider subsystem. For an ISC, the culture change process involved in providing the decider with knowledge and decision-making capabilities comprises the various activities involved in fostering a culture, that is, the ISC fostering process. The ISC fostering process is therefore a very necessary part of the forming view of ISC from a GLS perspective.

The fostering process is designed to align the actual ISC with the desired ISC. This means that it is a process which makes decisions to trigger processes and activities which will result in the plan/charter for the system being fulfilled. How this is done will now be briefly discussed.

Fostering a strong ISC involves aligning the ISC dimensions (as previously explained in section II). In order to foster a culture and align the components of an ISC, change is required. Change is not uncommon within an organization, as it is necessary to ensure its continuity. Schein recognized the necessity of the change process at a cultural level [7]. He therefore proposed a structured change management process which aimed to facilitate an organizational culture change. Many authors have adapted this culture change; this paper will use an adaption discussed by Okere, Van Niekerk and Carroll [16].

This structured change management process consists of eight steps (shown in figure 2). These steps are as follows:

1. Obtain top management support and commitment. This is the stage in which (as a response to a specific business problem and context) the top management levels are decided to gain an understanding of the existing cultures, and acknowledge and commit to any existing necessary changes [16]. In order to accomplish this, management’s understanding of the culture would require knowledge of the existing culture’s existing AFs, EVs, SAs and KN. Only then could management declare new espoused values.

2. Define the specific business problem. This is the stage in which the current culture is analyzed and the preferred new culture is defined. The gap between the two culture states is also analyzed and the required steps to start the needed transformative process (unfreezing, learning and refreezing of concepts) are defined [16]. This is the stage in which the current and desired ISC dimensions would be compared.

3. Develop strategic action plan. This is a self-explanatory stage in which plans for the many steps within the transformative process are planned, for example the identification of required action and behavior changes, education plans, awareness and support encouragement [16].

4. Create a cultural fit. This is where a cultural fit is facilitated using mechanisms such as education, training and reward systems [16]. This stage would be where the actual execution of the plans and decisions would begin. Further, more detailed, implementation would then be executed via the next four stages of the process.

5. Develop and choose a change leader team. This is the stage which ensures that the individuals involved have a common purpose [16]. This could happen at a single or multiple levels of the culture.

6. Create small wins. The stage where important actions and steps within the process are identified as markers that will indicate the desired culture change [16]. These markers are used to motivate employees [16]. One of the aims of this stage would be to try involving everyone in the fostering process.

7. Identify metrics, measures and milestones. This involves the identifying of metrics to measure success and track change [16]. This stage logically follows its predecessor and aids in determining whether the decisions being made and implemented are having the desired result.
8. **Feedback and review.** The receiving of indicators from internal and external factors that may indicate the state of the culture and whether further change is required [16]. Indicators should include new measurements and estimation of SA, KN and AFs which have resulted or changed because of the changes made to comply with the EVs.

This change management process is the desired decision activity that aids the alignment of an ISC’s dimensions. The entire change or culture fostering process is a continuously iterative, scalable model which may be applied within many a context. This process is an essential component of a living ISC system, as it enables all ISC living system activities and communications. Without this process the ISC would not be a living system as no communication would occur between ISC dimensions.

Besides being the charter and decider subsystem, this aspect of an ISC fostering process is also what enables another of a living system’s characteristics, namely, its ability to self-repair and self-maintain. This characteristic will be briefly explained by the next section.

C. **General living system can self-repair and self-maintain**

One characteristic of living systems that is particularly important is its ability to self-repair and self-maintain provided the necessary components are in place. This is an important and necessary characteristic in order for a system to maintain a level of constancy over time [6], [15].

Within a living biological system self-repair and maintenance take place according to the following points: information processing, energy processing, material processing, synthesis of parts by combining materials, rearrangement and connection of disarranged parts, energy storing for fuel reserves and necessary structure, and removal of worn parts [6]. In a non-biological living system this can be similarly identified in the fostering process of an ISC (discussed in previous section). To ensure that an ISC corresponds with the organization’s overall target and the targets of the various other subcultures, an ISC must be created, maintained and changed continuously [1]. How these map to one another will now be briefly explained.

Firstly, the synthesis, rearrangement, removal and replacement of parts indicates that, at this point, aspects of what works in a system are combined with other aspects that work from the same or another system, thereby replacing components that do not work and are no longer required. In the ISC fostering process this would occur throughout the entire process, while the process attempts to change/evolve the existing ISC and its components into the desired ISC and its desired components. For example, in an ISC fostering process, as previously discussed, the existing SAs, KN and AFs may start to be examined for compliance with the EVs of the desired ISC. The components of the existing dimensions that complied would then be then reused and possibly modified and/or expanded upon. This process could potentially mesh components from multiple implementations of the ISC (to be explained in section E) so as to obtain the best result.

Within the detailed implementation of this process it could be argued that the artefacts and resources allocated to the culture-fostering process would be equivalent to the energy, information and material needed for the system’s processing activities. This would include all the activities and resources allocated, expended and created within the processes to alter the AFs, SAs and KN to match the ISC’s desired EVs and other components. The resultant ISCs at the various levels of the living ISC system would be considered the energy stored for fuel reserves and the necessary structure, as this is what will facilitate future changes while itself being the existing cultural structure/product. A further in-depth examination of how exactly the resource allocation, use and processing activities map to the GLS processing activities will form part of future work.

The EVs, SAs, AFs and required KN change as the people, processes, technologies and suchlike governed by them or generating them change. This is taken into consideration within the fostering process by means of the feedback process. Therefore, they are considered part of the ISC— not external to it. Taking this into consideration, as well as the self-repair and self-maintenance points discussed, it is clear that an ISC is capable of, and is already, self-repairing and self-maintaining. The fostering of a culture entails the repairing and maintenance of that culture. However, whether the fostered ISC stabilizes and is adopted in a manner which ensures that the culture remains in a state that aligns with the desired EVs and so on is debatable. This debate will be addressed in future work.
Having now discussed the abstract charter (planned), and the decisive and self-maintenance characteristics of a culture, it is now necessary to understand the characteristics of a living system that actually implement/execute what is facilitated by those that have been previously discussed. The first of these characteristics to be discussed details the way a culture, as a system, works.

**D. General living systems are open systems with significant inputs, throughputs and outputs of various sorts of matter – energy and information.**

This section will provide the simplest explanation possible for how an ISC, on a functional level, exhibits the classic behavior of a living system. Firstly, an understanding is required of how a GLS functions.

Any GLS system is defined by its boundary. All system activities occur within the system boundary; anything outside it is considered the system’s environment. Within the system boundary a constant flow of information, energy and matter into, through and out of the system is maintained [6]. This flow enables the system to fulfill its purpose. Living systems import matter/energy, as well as information, as input from its environment [6]. What is included in the types of received input is generally selective (relevant to systems purpose). These inputs are then used in the system’s throughput (“metabolism”) process.

In biological living systems this metabolism consists of thermodynamic energy processing and information processing [6]. The thermodynamic energy processing component of the metabolism format provides the “energy required for important activities such as reproduction, production and repair” [6]. The information processing aspect of the metabolism enables continuous information exchange over the system boundary (information processing). It is the information processing and each system’s focused programmed decisions which help to regulate, adjust and control the way the thermodynamic processing occurs [6]. As a result of this, information processing therefore regulates the system’s internal stresses and external strains, while allowing the system’s purpose to be fulfilled [6].

During the metabolism/throughput process the system obtains/creates what it needs as well as some products or by-products. The system’s purpose is fulfilled when the processing (throughput and transformation) creates a product which is specific to the system. Thus, once the internal processing procedures are complete, the system exports its specific product output into the system’s environment where it is absorbed or collected by another system [6].

The GLS system will maintain a steady state of negentropy even though entropic changes occur in them. This happens because they take in inputs of higher complexity or organization or negentropy than their outputs. This difference permits them to restore their own energy and repair breakdowns in their own organized structure. This is a continuous process because, while the system releases its output, it simultaneously absorbs new input (matter/energy/information) from the resources in the environment [6]. This reabsorption of energy allows the system to continue its metabolism, self-maintenance, and self-repair processes.

In summary, a GLS functions by absorbing inputs from its environment, processing these inputs within the system boundary to obtain/create what the system requires, and then re-feeds any products or by-products of the processing back out into the systems environment [6]. This functional process can be found in the operation of an ISC.

In an ISC, the culture has expected inputs, namely, the EV and the SA and the existing culture’s AFs (mostly the daily work process). These inputs are absorbed into and processed in the ISC fostering system. The EVs come from top management and the SAs come from the employees or users. Both the EVs and the SAs may be considered the information inputs absorbed by the system. They are processes and they regulate the ISC’s process, which is equivalent of a GLS’s thermodynamic processing. The existing culture’s AFs, such as the daily work processes and procedures, are the equivalent of a GLS’s matter/energy input imports. The processing of them to create a more secure culture for this system’s particular context that meets the requirements within the EVs, which were its input, is the ISC’s equivalent thermodynamic processing. The products which are created within the ISC system are role-based business behavior processes, and procedures which are not secure according to the current cultures EVs, SAs and KN. The conceptual map of how this processing occurs is shown in Fig. 3.

![Figure 3: The input, throughput, output process of a living information security culture system](image-url)
fostering process in this format would depend on the context in which the ISC is being fostered.

An ISC is not a single implementation of a concept. Instead, it is multiple implementations of a concept, in different contexts, which together fulfill the overall system’s purpose. This existence maps to the nested system characteristic of a GLS, which will be discussed in the next section.

E. General living systems are nested, unitary systems

All living systems consist of similar molecules or components and show an evolutionary progression toward increasing complexity [15]. Essentially what Miller meant by this observation is that all living systems tend to exist as composites of other simpler living systems. Therefore, a living system is a hierarchical suprasystem of its subsystems, which are integrated to form actively self-regulating, developing, unitary systems with purposes and goals [6] [15].

Miller originally identified eight real and concrete hierarchical levels at which hierarchical levels could exist. The eight levels compound as follows: Cells>>Organs>>Organisms>>Groups>>Organizations>>Communities>>Societies>> Supranational. Each new level is more differentiated and considered to be higher than its predecessor; and is composed of all lower-level systems [15]. The vital system components of one level are systems in their own right on the level below. Therefore the larger system is typically the subsystem’s environment. The lack of physical cohesion among the components of a living system increases with the level’s complexity, but is often compensated for by advanced communication systems which tie the components together [6].

Each level has its typical individual structure and processes. They serve their own purpose which is self-contained while also contributing to the fulfillment of the purpose of the host’s larger system. Each system (as discussed in the previous section) takes in inputs that are required selectively for the system’s purpose; it then performs its own contextually influenced activities and processes, and outputs products into its environment. The products are then absorbed by another system that selectively requires them for its own throughput processes. This process continues throughout the nested system’s levels and hierarchy.

Typically, the literature seems to indicate that organizational culture and its subcultures such as an ISC operate as an overall construct [10]. This construct has been perceived to operate as a solid, single-levelled formal culture. However, the authors do not believe that culture can be considered that simple. Rather, they would like to propose that an ISC is a multileveled composite of nested ISC sub-cultural constructs. Moreover, they would like to propose that an ISC’s implementation depends mainly on what business problems are being solved and what the security requirements of that process are, as well as on the business process it surrounds and the stage of the workflow process it is in.

A business process will typically work across multiple departments. Therefore, such a process will circulate throughout parts of the organization’s main business process. The business process is therefore a large component of the culture surrounding it. The entire organization has an organizational culture and components of this culture are implemented by some/all of the organization’s subcomponents, for example departments. Similarly, the ISC, which is also a component of the organizational culture, would have different aspects which are applied in varying degrees within the various departments, because different levels of severity or priority according to the status of the process stage will exist within the specific environment. Cultures are in a sense context-sensitive. Since the ISC is a subculture of the organizational culture, it must sometimes adapt to trade its best practices for secure practices which best facilitate a secure business process in a particular context; these “trade-offs” have always been necessary[4]. Examples of some contextual factors which may necessitate such trade-offs include the role being played by the user or department, as well as the nature, purpose and priorities of the current task being performed [14]. The implementation of an ISC may therefore occur differently within the different departments for their own contributions to the different business processes and their different stages. This may be represented as a nested system of cultures surrounding various work processes which form the artefacts of an organismal culture. This is illustrated in Fig. 4.

Fig. 4 illustrates how subcomponents of an ISC can have the same goal, but be implemented separately. This illustration will be further clarified through the use of a real-word ISC example.

Within the example’s organizational context, one of the espoused values could be that there must be a strong secure password culture. So the employees in every organizational role are provided with the necessary knowledge (KN) about how to create and manage a password securely. Gradually, the employees develop SAs and AFs which reflect their acceptance and this, in turn, aids the development of a strong, secure password culture. However, what this type of culture is and how it is implemented may be vastly different depending on the particular version of the culture’s context.

If System A were the financial department it might have a number of extremely important password-protected work activities. These activities may consist of multiple stages of implementation and, because of their importance within the department, require high security practices to protect their integrity and confidentiality. Therefore, within the financial department a strong, secure password culture would surround this work process. In this example, the password would enable only one employee to access the folder at a time, and they would have to change the password often to prevent unauthorized employees within the department from accessing the information being protected. However, this work process consists of multiple stages and may require input from multiple departments. Therefore, file involved in the process may move to another system, for example ISC System B, which for this example would represent a human resources department. A stage in this work flow process may require multiple employee details as input into its product. However, the secure password culture might differ in this department. It could be that many people in this department need to be able to access the file at any given time. Therefore, in this department all the employees share the password for the process. Moreover, the department
may only define the password as not being secure if someone external to the department knows the password.

Figure 4: Nested ISCs following a work process

This example is illustrative of a simple scenario. In reality, a scenario may be far more complex, with multiple stages of a process being accessed during a single business workflow, with its importance within the implementation of the ISC varying between systems and even departments.

In summary, an ISC would be very environment and context sensitive. Thus, its visible AFs would differ in accordance the following environmental and system factors: organizational work process, department, priority of process stage within the department, and the department's existing ISC. A living systems view might have many other implications and these will be addressed in future work.

V. CONCLUSION

This paper has shown that an ISC exhibits, and can be mapped, to five primary characteristics of a general living system. This conceptual mapping indicates that it is possible to conceptually consider an ISC to be a type of general living system. As such it is likely that all/most general propositions associated with all living systems (regardless of size, origin and complexity) are true for ISCs. Therefore, it may be possible to further identify and manipulate the general processes and basic understandings of general systems theory within an ISC. Information security specialists as well as organizational employees may therefore potentially be able to track, monitor and manipulate their ISC based on context-specific occurrences of these GLS prepositions. Lessons learnt from GLS theory could potentially be applied to the fostering and maintenance of ISC. This would also provide tools to further clarify the nature of an ISC. The ability for any employee to understand the ISC as it applies to the specific context of his/her own role could be advantageous for the fostering, management and general understanding of the ISC. This general systems theory view of ISC may therefore have implications for all the above-mentioned ISC activities, as well general organizational activities and cultures. Future work will focus on applying such a viewpoint practically in order to evaluate the utility of the GLS view for the purposes of managing an ISC. Additionally, the remaining subsystems of GLS will be mapped to ISC.

REFERENCES

From Information Security to Cyber Security Cultures

Organizations to Societies

Rayne Reid
School of ICT
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
s208045820@live.nmmu.ac.za

Johan Van Niekerk
School of ICT
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Johan.VanNiekerk@nmmu.ac.za

Abstract—Currently, all Internet and ICT users need basic levels of cyber security awareness and knowledge to perform their daily activities securely. Many security specialists and, indeed, nations are acknowledging the need for populaces to be aware of and educated about being more cyber secure. To achieve cyber security in current populations and to ensure continuity in future populaces, a “self-renewing” belief which affects behavior is needed. In an organizational context this need is met through the fostering of an information security culture (ISC). Similarly, in a societal context a cyber security culture (CSC) ought to be fostered. This raises the question of what precisely would constitute a CSC and how it differs from an ISC. The objective of this paper is to propose ways in which a CSC may be defined and viewed in comparison to an ISC.

Keywords—information security culture; cyber security culture; definition; human factor

I. INTRODUCTION

In today’s information-centric society the securing of information for information communication technologies (ICT) and ICT users has become of paramount importance. Organizations have long acknowledged this, and have consequently implemented suitable information security solutions. Unfortunately, many of these information security solutions are innately flawed, as the components of such an information security solution and its management involves processes, technology and people [1]. Although processes and technologies can be created to be theoretically secure, how truly secure they are depends on the people involved in their use and implementation [2]. Furthermore, whether people use the technologies in a secure manner and follow the secure processes completely and correctly can drastically affect the extent to which these components are secure, because people can consciously and unconsciously become a threat to any information security solution [3]. As a result of this failing, many authors acknowledge that the people involved are the weakest link in information security [2]–[6].

To counter this human factor, researchers suggest as a solution the fostering or development of a culture of information security [3]–[5], [7]. An information security culture includes all the socio-cultural measures that support technical security methods, so that information security becomes a natural aspect of the daily activity of every employee [8].

Organizations have thus for a while now been fostering an information security culture (ISC) within themselves. These ISCs have been widely accepted as viable counters to “human factor” threats in information security. However, merely fostering such cultures in an organizational context is no longer sufficient to protect the majority of users. Moreover, the need for information security is no longer considered to be solely an organizational issue.

The world beyond organizations has become and continues to be progressively more information-oriented. This means that the average citizen is increasingly being exposed to related risks and threats targeting their transactions, information and own selves. The risk of the average citizen being exposed to the technologies and their associated risks has therefore increased. Consequently, information security principles have become applicable to information use in a personal context. Currently, all Internet and ICT users need basic levels of cyber security awareness and knowledge to perform their daily activities securely.

Security issues relating to the cyber-world require a coordinated and focused effort from national and international society, governments and the private sector. To suit this broader security context a security solution with a greater scope than organizational information security is required. Many security problems primarily exist outside an organizational context, affecting individuals who use the web in a private or social context. Cyber security is thus a solution which focuses on this all-encompassing broader context.

Cyber security is the protection of the interests of a person, society or nation, including their information and non-information-based assets that need protection from the risks relating to their interaction with cyberspace [9]. Humans and their societies are part of the assets needing protection. Many security specialists and nations are now acknowledging the need for populaces to be aware of and educated about being more cyber secure. To achieve this within current populations, and ensure continuity within future populaces, a “self-renewing” belief which affects behavior is needed. In an organizational context this need is met through the fostering of an ISC. Similarly, in a societal context a parallel cyber security culture (CSC) ought to be fostered. This raises the question of what precisely would constitute a CSC, and how does this differ from an ISC.

The objective of this paper is to propose how a CSC may be defined and viewed in comparison to an ISC. This paper
will aim to meet this objective by, firstly, demonstrating the need for a cyber-security culture in current society; secondly, examining what known views of information security exist; and thirdly, determining whether cyber security differs from information security. Finally, the paper will conclude by identifying which components and considerations of a CSC will differ from their predecessors.

II. METHODOLOGY

This paper presents a comprehensive literature review of sources relating to ISCs and CSCs. ISCs will be the primary focus as limited literature exists. An argument using the review’s findings and logical inferences will then be presented to differentiate a CSC from an ISC.

III. BACKGROUND

The adoption of innovations by society at large is described by the diffusion of innovation theory. This theory explains how, why and at what rate new ideas and technologies spread through cultures [10]. Additionally, it explains the consequences of such diffusion. These consequences can range from positive to negative. To determine whether a particular consequence is positive or not a number of characteristics of the consequence is examined. These characteristics result in the consequence being categorized into one of three categories: desirable versus undesirable (functional or dysfunctional), direct versus indirect (immediate result or result of the immediate result), and anticipated versus unanticipated (recognized and intended or not) [10]. These consequences directly affect the society within which the diffusion of the innovation took place.

In the past the adoption of technological advances, such as the car and airplane, caused major changes to occur within society. These advances had many direct, anticipated and desired consequences. In the case of the car people gained a reliable means of personal travel, they could travel further with fewer inconveniences than before and many business opportunities arose from this. However, these benefits were sadly accompanied by problems. Some of these problems included risks to safety, trade and continued productivity. Car accidents could occur if pedestrians or other cars were not considerate of one another; the conditions of roads affected where people were willing to travel; businesses began to invest more in services that made use of the innovation, rather than those that did not; and finally crimes targeting the technologies came into existence, for example car theft and vandalism. To counter or prevent these risks society had to adapt and accommodate the technology in daily life. Thus indirect and unanticipated consequences of the adoption of the technology included society taking measures such as creating road safety laws; committing to improving and maintaining infrastructure that supported or developed the technologies, for example road maintenance; and the drafting of legislation to account for the crimes relating to the technology. In brief, past technological innovations such as cars have had a major impact on society, changing it forever. Currently, the wide adoption of cyberspace is having a similar impact on society.

The diffusion of cyberspace into society has occurred rapidly over the past few decades. Consequently, many changes have occurred within society to accommodate the Internet as well as ICT. Subsequently, as predicted by the theory of the diffusion of innovations, many positive and negative changes have occurred within society as a consequence.

Cyberspace is an integral part of modern-day society. It is a highly effective tool and enabler of activities. It influences or is integrated (observably and inconspicuously) into all facets of most people’s daily lives and digitally transposed activities [11], [12]. Consisting of ICT, cyberspace has become part of the critical infrastructure that supports socioeconomic growth, the governing of nations and sub-societies, the conducting of business and the exercising of human rights and freedom [11]. As part of its desirable and anticipated consequences it has enabled businesses and governments to generate income and employment, provided access to business and information, enable e-learning, and facilitated government activities [11]. As such, the Internet and ICT have become indispensable and have facilitated many positive aspects of the modern way of life. Conversely, however, user adoption of these technologies has also enabled less desirable activities, risks and threats such as information exposure, crime, espionage, terrorism and warfare to make use of these same infrastructure [13].

Subsequently, cyberspace, like technologies such as the car before it, is resulting in a period in which society must adapt to the undesired, indirect and unanticipated consequences of its adoption. In the context of cyberspace and technology adoption, one such consequence which is important for societies is the adoption and use of the measures that have to accompany threats and risks. These most commonly relate to the implementation of information and cyber security. It is unlikely that the adoption of cyber security practices will completely negate the risks posed by such undesired consequences; however, they may greatly mitigate the risks.

A. Information and Cyber Security

Information security is a process involving the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk and maximize return on investments and business opportunities [14]. It involves the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording and destruction [15]. The overall objective of information security is the preservation of the confidentiality, integrity, and availability of information and information resources [16]. The protection of these characteristics has become an essential tool in the maintenance of any competitive edge, cash flow, profitability, legal compliance and commercial image to be gained or derived from the ownership of information [14]. Comprehensive information security solutions involve multifaceted physical, procedural and logical forms of protection for the information in question. This type of security is typically implemented in an organizational context [17].

The concept of information security and its relevant practices and procedures is constantly evolving to suit the fluid business environment. However, the mere implementation of
information security solutions by organizations is insufficient [12]. The world outside of organizations has become progressively more information oriented and, as a result, information security principles have become more applicable to information use in a personal context. At present all Internet and ICT users need to have at least a basic level of cyber security awareness and knowledge in order to perform their daily activities securely [5], [18]. Security issues therefore now require a more coordinated and focused effort from national and international society, governments and the private sector [19]. This has led to the defining of another type of security, namely, cyber security.

Sharing much of the scope of information security, cyber security principally involves the protection of information and ICT; however, its scope also extends much further [9]. Cyber security involves the preservation of the confidentiality, integrity and availability of information in cyberspace [9]. Cyberspace is a “complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form” [9]. Therefore, in actuality, cyber security involves the protection of the interests of a person, society or nation, including their information and non-information-based assets that need to be protected from risks relating to their interaction with cyberspace [20]. As the definition of cyber security states, “humans and human societies have grown to become part of the assets that need to be protected” [20]. Therefore, as with information security, humans are still considered to be both a threat and a vulnerability; however, in cyber security they are also considered to be an asset needing protection in cyberspace [9].

Thus information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities [20]. Comparatively, cyber security is the protection of cyberspace itself, as well as the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace [20].

Traditionally, organizations have implemented some form of protection for information resources in the form of information security. However, as the boundaries of information usage moved beyond the organizational context, so too did the associated risks. Subsequently, within this larger societal context, based on the previously discussed definitions, the need for information security has largely been superseded by the need for cyber security.

ISO/IEC 27032 (2012) and the previously discussed definitions all indicate that the boundaries of cyber security and the risks it protects against are greater than those of information security. In a societal context (which encompasses organizations and individuals), the risks and threats faced by users are more encompassing than those addressed by typical information security. Therefore, in a societal context it is necessary to look beyond the organizational information security boundaries. The incorporation of cyber security solutions into society is the area of study for this research.

Most previous security-related research dealt with information security, not cyber security. Additionally, the majority of this research was conducted within an academic or organizational context. However, it would be prudent for researchers of cyber security to take heed of lessons learnt from information security, because cyber security still overlaps significantly with information security. The terms “information security” and “cyber security” are also often used interchangeably in the literature. Therefore, although this research focuses on cyber security, of necessity it also examines the literature relating to information security.

B. The Need for a Cyber Security Culture at a Societal Level

Siponen (2001a) states that all users who are involved with any form of ICT or services, particularly in an Internet environment, need to have at least some level of information or cyber security awareness. This statement indicates that users both within and outside organizations need to be cyber security conscious. Subsequently, having organizations as the sole primary practitioners of information security practices and awareness was not deemed sufficient to meet all of these users' needs. Siponen identifies five security dimensions of awareness, and their key issues, that needed to be addressed in order to meet all users’ security needs. These dimensions include the organizational, general public, socio-political, computer ethical, and institutional education dimensions [12]. The raising of awareness in all of these dimensions could lead to a cyber security aware culture within an entire society.

The need for cyber security practices and awareness outside of organizations has been further proven over the past decade. In current society, governments in several countries (including the United Kingdom and the United States of America) have recognized the many potential benefits that the adoption of the Internet and ICT may have for their country's welfare [11], [21], [22]. Therefore, in many of these countries citizens are being actively encouraged to adopt these technologies. Unfortunately, although these pro-technological progress movements are having some positive results, they are also having some unintended consequences. One of the most prominent problems is that these societies are establishing a trend of becoming increasingly technology dependent whilst also becoming increasingly vulnerable to cyber threats [23]. This is because many users are not significantly aware of or secured against the cyber threats targeting them via the adopted technologies. This alarming trend needs to be corrected. A potential approach to alter this trend is attempting to foster a culture of security awareness.

Ultimately, entire societies need to be security conscious. Consequently, as part of the socio-political dimension many countries' governments are beginning to recognize that the socio-political and cultural necessity of cyber security awareness is an important factor in the wellbeing of their citizens [12].

Cyber security has become a matter of global interest and importance. Currently, different countries already have different states of security awareness. Increasing their states of security awareness for their national, corporate and citizen safety is unequivocally important for all countries [18]. Thus it is becoming vital that organizational and general users all receive proper security awareness training as soon as possible, in order to reduce the security risks to themselves and to other countries [18]. Already more than fifty nations have officially
published and begun to implement some form of cyber security strategy [11]. Several countries are beginning to implement national cyber security solutions so as to actively encourage their citizens to become cyber security aware. The implementation, maintenance and improvement of these national cyber security solutions comprise a vast range of components, ranging from the operational/administrative level to the tactical [11].

The starting point in each of these efforts is the government showing its commitment to the cause by drafting a national cyber security strategy and other documents of a political nature (laws, regulations, technical and operational protection measures etc.) [11]. Thus the first component of the solution deals with the prescribing of physical, technical and operational controls [9]. However, a true cyber security solution requires more than these controls. This is because the issue of the human factor in security has become increasingly prominent alongside technical issues [24], [25]. Cyber security recognizes the people (human factor) involved with the solution as simultaneously assets, threats and vulnerabilities. It is therefore vital that this component of a cyber security solution is specifically dealt with.

In an organizational context, most current approaches to addressing this human aspect of information security agree that an information security culture should be fostered among users [26]–[28], as this is vital to the success of information systems governance, risk management and compliance [29]. Within the context of a national solution the scope of the human factor would be even greater; however, the solution may be theorised to be similar. Therefore there is a need to foster a culture of cyber security awareness within society.

This raises the following questions: “What constitutes a cyber-security culture?” and “How does it differ from an information security culture?” To begin to address these questions the following sections will firstly examine ISC as a concept and will then identify the way in which a CSC and an ISC would differ.

IV. HOW A CYBER SECURITY CULTURE DIFFERS FROM AN INFORMATION SECURITY CULTURE

A. Information Security Culture

Culture is broadly considered to be the overall, taken-for-granted assumptions that a group has learnt throughout history [30]. It emerges over time and is visible in views and actions which reflect a belief [4]. ISCs build on this premise.

Organizations have acknowledged the need for an ISC within a business context. In the past it was found that the technical and procedural components of an information security solution were not in themselves sufficient to address the human aspects of information security [5]. This led to the recommendation that security be embedded in the organization through the institutionalization of information security. Von Solms called this the Third Wave of security [5]. One aspect of this institutionalization of security involved cultivating information security as a corporate culture; that is, information security standardization; international information security certification; the implementation of metrics to continuously and dynamically measure information security aspects in a company; and finally, the cultivation of an information security culture as a corporate culture [5]. These recommendations have since been and continue to be implemented, improved and researched.

Many authors have dealt with the topic of ISC ([2][31][4], [32], [33]). Most of these authors focused on cultivating, assessing or auditing a culture. To achieve this, the authors had to explain what they considered an ISC to be comprised of. Literature shows that they commonly based their understanding and representation of an ISC on adaptions of Schein’s three-tier organizational culture model [8]. The tiers of Schein’s organizational culture model consist of underlying assumptions, espoused values and artifacts [30]. However, this model deals with organizational culture in general, not ISC specifically, and Schlienger and Teufel seldom provide in-depth explanations about how their interpretation of the adapted model translates to the context of information security. This left much about the practice to be subjectively interpreted. Van Niekerk and Von Solms bridged this gap by presenting a conceptual model of an ISC which expanded on Schein’s model and focused on explaining how the culture’s underlying components and processes could influence one another [6].

Van Niekerk and Von Solms’s definition of ISC derives from and expands Schein’s organizational culture model. Schein lists artifacts, espoused values and knowledge as dimensions of his culture model [30]. Van Niekerk and Von Solms expanded the ISC model by concretely integrating the requisite underlying information security knowledge as a separate component in their model [30]. This knowledge dimension was included as the authors theorized that in order to foster an ISC successfully (as a subculture within an organizational culture), all business activities would need to be performed in a secure way [33]. Adequate information security knowledge and skills were therefore deemed a necessary requisite to enable an employee to be able to perform any business activity in a secure manner [6]. Accordingly, their conceptualization (as shown in Fig. 1) of an ISC consists of four information security-related components, namely, artifacts, espoused values, shared tacit assumptions and knowledge [6].

The exact contents of each of the other dimensions were also slightly altered in order to be more context-specific to ISC. The ISC-specific interpretation of the model dimensions therefore now refer to the following framework components:

1. Artefacts (AF) – Detailed procedure of the organization’s daily tasks. This dimension includes the visible structures and processes which were deemed to be “measurable but hard to decipher” [6]. Examples of these would be the architecture and security mechanisms of the company, as well as information security policies and procedures.

2. Espoused Values (EV) – The guidelines for what to include in a policy, and subsequent ISC to adequately address the business’s needs. These include information security strategies, goals and philosophies. In brief, the information security-related espoused justifications and official viewpoints [6].
3. **Shared Tacit Assumptions (STA)** – The beliefs and values of the individual and collective employees. This includes their unconscious, taken-for-granted beliefs, perceptions, thoughts and feelings. In brief, it is the layer at which the people are involved and as such it is the ultimate source of values and action [6].

4. **Knowledge (KW)** – The necessary and required levels of information security-specific knowledge needed to perform the daily business tasks in a secure manner [6].

![Figure 1: Levels of culture. Adapted from Schein (1999, p. 16) [6].](image)

This adoption of Schein’s organizational culture was very suitable for an ISC. This is because thus far the literature has dealt with ISCs that were cultivated, assessed, audited and so forth in an organizational context.

However, in terms of this CSC research, the use of Schein’s model may be questioned and requires further justification. Schein’s model depends on its organizational context and an understanding of how a culture can be cultivated or measured within this insulated environment. The previous section has shown that cyber security extends beyond the contextual borders of an organization. This extension of scope will likewise affect the CSC. Therefore one should ask whether Schein’s model is acceptable for use with a CSC, or would other models such as the one offered by Hofstede [34] be more suitable. The next section will examine these considerations as well as others for a CSC.

**B. Considerations for a Cyber Security Culture**

All of these previously mentioned ISC models focused on an ISC in organizations. This paper aims to address the ISC needs of a society. The previous sections established that a CSC will likely be similar to an ISC; however, there will be some definite differences. This section will examine some of the differences that exist and the considerations that have to be made. The issues that will primarily be discussed relate either to the CSC’s context or its components.

1) **Context**

The first significant difference between an ISC and a CSC would, as the previous section noted, be the context in which the culture would be fostered. Information security cultures are cultivated and managed within insulated organizational contexts. This context translates to being a relatively well-controlled environment with relatively predictable user behavior, activity and profile sets. Comparatively, with the scope of a cyber-security solution the culture would be cultivated within a societal scope. The environment within a societal context would likely be less controlled; user profiles would range across many skillsets, age ranges and other variables; and the activities being performed by the users would be less predictable than those within a purpose-based organization.

These differences would affect the ease with which a culture could be established and the degree to which the users may be willing to subscribe to the culture. It is probable that attempts to foster an ISC may experience faster and more complete success than attempts the foster a CSC in society. This is because organizations tend to have a number of cultures or behavior sets which they seek to instill within their employees. It is possible that employee exposure to a number of such continuous culture fostering processes with a particular (arguably regulated) environment may make them more amenable to accepting other cultures in the same environment. Comparatively, a societal context is less closely regulated. For example there are broad-based culture systems, such as national culture, religious culture etc. and even smaller community cultures, which are less regulated than those within a work environment. Therefore the users are more likely to be individualistic than when they are in their work environment.

Within the context of an ISC, Furnell and Thomson identified a number of factors that could be theorized as affecting the users’ (involved in a solution) willingness to comply with the culture [2]. These factors may also affect whether a societal user would be willing to accept a cyber security culture. The factors which should be considered for the CSC are the following: the roles the user must play; the nature of the task; user behavior and the psychology of the users [2]. How the various elements of an ISC and a CSC will differ will now be briefly discussed.

The role, current task and user behavior that the users must adopt from a security perspective while completing their tasks would relate to who they are and what they are doing [2]. Within the context of an ISC this role would relate to what the users are actually expected to do as part of their job, and their security responsibilities required by the job. Within this context the role should be easily defined, as a user will be goal/task oriented to the organization’s work process. Therefore, a user will only be expected to consider their role and responsibilities for their part of the task. They would not be expected to know how to fulfill the roles outside their own job description. For this user the number of roles they may play will thus be limited and they will only need to adopt the culture pertaining to these limited roles. In comparison, in a personal capacity within a societal CSC, the number of roles a user may play will be dependent on the activities they as an individual elect to complete. The user may have some fixed tasks as well as many ad hoc tasks which have varying contexts. This means that a user within a CSC would need to be exposed to a broad culture which shows them how to adapt their roles based on a task. This factor also relates to the
general user profiles involved in the culture. Within an organization, certain age ranges, skillsets and suchlike are expected and thus their roles relate to these characteristics. However, when in open society the types of role characteristics are infinitely combinable.

Having now determined how the contextual considerations that will affect the consideration of a CSC, the next subsection will establish how the components of the cultures will differ.

2) Components

As a result of the comprehensiveness of Van Niekerk and Von Solms’s definition of an ISC [6], the focus on the conceptualization of an ISC and the degree of similarity of the degree relative to the explanation to a CSC as well as the ISC, this paper will adopt their definition of an ISC to discuss the similar aspects of a societal CSC.

As discussed in the previous section, Van Niekerk and Von Solms conceptualized an ISC as having four component levels, namely, Artifacts (AF); Shared Tacit Assumptions (STA); Espoused Values (EV) and Knowledge (KW). In the context of a CSC it is likely that similar abstract components would also exist. However, how they translate within real-world applications as artifacts and behaviors will differ due to the scope of the context. This section will briefly examine how these cultural components could emerge differently.

The first component to consider would be the EV. Typically, within an ISC the EV describe the values that an organization is said to be advocating or promoting [35]. In the context of an ISC, these EV would be issued by the board of directors or the high-level management on the business's behalf. They would manifest in the business's information security policy, and the business's general vision. This is in an organizational context, but within a CSC the approach would be similar. In terms of the overall societal scope a similar top-down approach would also be necessary; however, the degree to which they may be hedged would likely be more dependent on the context and the users involved than it would within an organization. In the broader society, the espoused values would likely be issued by governmental, national or international agencies and would then manifest as a national cyber security culture. This would be similar to what occurs in the ISC. However, how a CSC may differ in EV is that, in societies, there are a number of sub-societies. And in these sub-societies, there may also be additional author representatives (i.e. top management), which may further issue other EV. These EV would build on the higher level specifications but may not contradict them. Essentially, the EV in a CSC would be notices such as rights, laws and national policies. Therefore they would cover very broad areas.

The second component to be considered would be the artifacts (AV). This component strongly relates to the espoused values. Considerations for this component are the following: Artifacts are the observed concrete or tangible behavior, or what an individual can see, hear and feel when they observe an organization. [35]. Therefore, in an ISC, examples of these would include the physical security, the information security policies and the procedures. In an organizational context these artifacts are capable of being very specific in their requirements. Comparatively, however, the artifacts of a societal CSC would likely involve national policy, laws and other recommended best practices. Owing to the nature of these potential artifacts, they would not be as easily established, or created to be as specifically detailed as an organization’s artifacts. This raises the question of how to communicate the more specific recommendations to the users in society.

The next consideration are the Shared Tacit Assumptions (STA) that are shared by a group of people and encompass the underlying thoughts and values that the employees of an organization believe to be true [35]. This level of corporate culture directly influences the behavior of employees that can be observed at the artifact level. In terms of an ISC versus a CSC, this level will be more easily measured or perceived in an organizational context. The STA among users in a society will exist; however, because users will also belong to sub-societies, they will develop individualized instances of STA. Therefore, in a CSC these STA will be more difficult to observe. Determining what STA exist will therefore be more difficult in a CSC.

Finally, the knowledge component will have to be considered. This relates to awareness of the requisite security knowledge needed to fulfill the user’s security roles while they are completing a task. In both an organizational and societal context the users cannot be expected to have such default knowledge. Therefore this component raises the question of how to provide the users with access to methods to gain this knowledge. Within an organization education and training is part of fostering an ISC. Education would likely also be used in fostering a CSC. However, what content should be included must be determined for the CSC, as the number of activities a user may need to perform securely is not as predictable as it would be in an organizational context.

This section discussed the primary/major considerations that would differentiate a CSC from an ISC. It was established that the components and implementation of a CSC within a societal context would significantly differ from the components of an ISC, although they would serve a similar purpose. It is the authors' belief that the CSC and the ISC are very similar; that the broader context of the CSC would have a major effect on the way a CSC is fostered in society compared to the way an ISC is fostered in an insulated organizational context. This theory will have to form part of future work.

V. CONCLUSION

The world’s rapid adoption of cyber technologies and services has exposed users to the many beneficial services and conveniences offered by the cyber world. However, it has also exposed them to many threats. Exposure to increasing threats and potential risks has led to cyber security knowledge and skills becoming a vital life skill for all cyber citizens. Therefore, as an important life skill they should be integrated into citizens’ daily cyber behavior to the extent that it becomes an unconscious action. A CSC should thus be fostered.

The literature has shown that many studies have been conducted and frameworks or guidelines for the fostering of
information security cultures proposed. These cultures are, however, confined to the organization’s environment and similar-sized insulated (controlled) environments. Nevertheless, compared to ISC, there are no widely accepted definitions or guidelines for what constitutes a CSC. To begin addressing this gap, this paper has proposed a conceptual understanding of the probable components and the consideration of a cyber security culture. Although the discussion presented here is not a definition of CSC, it does identify the questions, components and considerations that should be taken into account when defining a CSC. One of the major considerations for a CSC would be its lack of an insulated overall environment, because societal boundaries are considerably broader than the organizational boundaries of an ISC. It is therefore the recommendation of this paper that cyber security not be defended as an abstract concept to be applied to all contexts. Rather is it is recommended that CSC be defined to suit particular contexts.

VI. FUTURE WORK

Forthcoming research will examine how to foster a CSC in various contexts.

REFERENCES


Towards an Education Campaign for Fostering a Societal, Cyber Security Culture

R. Reid and J. Van Niekerk

Institute of ICT Advancement, Nelson Mandela Métropolitain University
e-mail: S208045820@nmmu.ac.za; johanvanniekerk@nmmu.ac.za

Abstract

The need for information security has moved beyond its traditional organizational boundaries. It is becoming a requirement for all information technology users. Many countries are recognizing this need for their citizens to be cyber aware and secure. Consequently these countries are beginning to implement national cyber security campaigns and efforts. Literature advocates that these campaigns should aim to foster a national (societal) cyber security culture to be truly effective. Currently there are no guidelines for how to foster a cyber security culture at a societal level. One of the elements required in a culture fostering process is education. This education needs to be effectively conducted to have a foreseeable, positive result which is measurable. Therefore a scalable, culture fostering campaign is needed. This paper reports a study of an annual cyber security educational campaign which aims to begin fostering a cyber-security culture amongst the youth in the Nelson Mandela Metropolis in South Africa. The objective of studying this campaign is to establish a baseline campaign from which suitable guidelines for a future campaigns (at any scale) may be abstracted.

Keywords

Cyber Security Education, Cyber Security Culture, Youth, Case Study, Awareness

1. Introduction

People, also known as the “human factor”, have been established as one of the weakest links in many information or cyber security solutions. These security solutions consist of technologies, processes and people. The technologies and processes within security can be created or drafted to be theoretically secure. However, how truly secure the technologies and processes are depends on whether the people use the technologies securely and/or follow the secure procedures.

People can consciously or unconsciously become a threat to any information security solution (Thomson et al., 2006). When they become a conscious threat it may be with a specific intent or via negligence. Alternatively when they become an unconscious threat it may be for a range of reasons including: a lack of knowledge of security practices; an inability to properly apply their knowledge to their own work role or environmental context; or common negligence. Regrettably as a result of this it is more likely that a breach within an information security solution will occur because of a human fault (the “human factor”), not a technical fault (Mitnick and Simon, 2002).
Within organizations the establishment of an information security culture (hereinafter “ISC”) has been widely accepted as a viable counter to this “human factor” threat (Van Niekerk and Von Solms, 2010). The fostering of a culture attempts to address two primary dimensions of the human factor: knowledge, and behaviour (Van Niekerk and Von Solms, 2010).

The establishment of an ISC has traditionally occurred within organizations. This is because in the past the integration of IT into daily activities, and the subsequent need for information security was considered more of an organizational issue. However, the perceived exclusivity of this issue is no longer a valid belief.

The world beyond organizations has become progressively more information-oriented. As a result information security principles have become more applicable to information use in a personal context. Thus at present all Internet and ICT users need a basic level of cyber security awareness and knowledge to securely perform their daily activities (Chen et al., 2008; Furnell, 2013).

Security issues relating to the cyber-world now require a coordinated and focused effort from the national and international society, governments and private sectors (Dlamini, 2009). To suit this broader security context a security solution with a greater scope than information security is required. Cyber security is such a solution.

Information security is a process involving the protection of the confidentiality, integrity, and availability of information from a wide range of threats in order to ensure business continuity, minimize business risk and maximize return on investments and business opportunities (ISO/IEC 27002, 2008). Cyber security also principally involves the protection of information and ICT; however, its scope also extends much further (ISO/IEC 27032, 2012).

Cyber security involves the protection of the interests of a person, society or nation, including their information and non-information based assets, which need to be protected from risks relating to their interaction with cyberspace (ISO/IEC 27032, 2012; Von Solms and Van Niekerk, 2013). Within this definition humans and their societies are part of the assets needing protection.

Many security specialists and nations are acknowledging the need for populaces to be aware of and educated about being more cyber secure. To achieve this within the current population, and ensure that it continues within the future populaces a “self-renewing” belief which affects behaviour is needed. In an organizational context this need is met through the fostering of an ISC. Similarly in a societal context a parallel cyber security culture ought to be fostered.

This paper represents an initial cycle in a larger action research approach. The paper begins to examine how a cyber security culture could be fostered via education. The findings of this study will begin to demonstrate how to structure a cyber security education campaign which targets needs of a subset of society. The next section will
provide further context and rationalisation for this study. This will be followed by the presentation of the study results, findings and conclusions.

2. Background

Culture is broadly considered to be the overall, taken-for-granted assumptions that a group has learned throughout history (Schein, 2009). ISC builds upon this premise. Many current authors deal with the topic of ISC (Schlienger and Tuefel, Da Veiga and Eloff, Van Niekerk and Von Solms). Most of these authors define ISC in terms of its underlying constituent components. This paper will use the definition offered by Van Niekerk and Von Solms (2010). ISC as an omnipresent concept understood by the people involved in the information security solution(Van Niekerk and Von Solms, 2010). They argue that over simplifying the ISC could be dangerous as an ISC consists of four information security related components:

1. Artefacts: The actual happenings within the organization’s daily tasks. This dimension includes the visible structures and processes which were deemed to be “measurable but hard to decipher”;
2. Espoused Values: The guidelines (strategies, goals) for what to include in a policy, and consequent ISC to adequately address the business’s needs;
3. Shared Tacit Assumptions: The beliefs and values of an individual and collective employees. This includes their unconscious beliefs, perceptions, thoughts and feelings;
4. Knowledge: The necessary and required levels of information security specific knowledge needed to perform the daily business tasks in a secure manner (Van Niekerk and Von Solms, 2010).

The accumulation of how these components develop and interact is considered to be an ISC’s effect (Van Niekerk and Von Solms, 2010). Each of these levels can either positively or negatively influence the overall ISC. It may be theorized that a cyber security culture would have similar components and behaviors, although the exact details would differ to some extent due to the practices differences in implementation details and context. The method by which the culture is fostered would be important.

A culture can be fostered through either coercion or education. Woodall (1996) argues that, if used, an equitable balance should exist between the degree of coercion used and the reward given, however, generally coercion should be avoided. Within an organizational context, users can be coerced into following security policies and procedures. This can lead to a forced organizational ISC. In a national context it is also possible to use coercion. However, due to ethical and implementation considerations it is a more difficult undertaking and thus less desirable as an approach. Within a national context the educational approach for fostering a culture is preferred. Educational campaigns to teach all of society’s users about cyber security issues and practices are thus required.

Many countries have recognized this need to become cyber secure. Part of the process of cyber-securing a country would be the education of the countries citizens about cyber issues and security practices. Many countries have acknowledged this
need for citizen education in their national cyber security policies (Klimburg, 2012, pp. 47). However, detail about how this education is to be provided to each society is not provided. This has led to a search for existing guidelines for such an endeavour.

A comprehensive literature review revealed that there are currently no widely accepted, documented guidelines for how to educate users at a societal level about cyber security. There are few generic guidelines for implementing cyber-security and societal educational campaigns even as separate subjects. This leads to two questions: “How can an effective cyber security educational campaign be developed?” and “How can this campaign be made suitable for educating an entire society?”

The first question’s solution can begin to be found through adopting some of the fundamental practices from the implementation of past (similarly purposed) information security campaigns. However, most information security education campaigns occur within organizations therefore the scope and its implementation would have definite difference. For example, in an organisational context education may often be formally (possibly mandatorily) conducted by security experts or human resources. Comparatively in a societal context such a practice would not be well-received. Therefore to answer the second question other methods are necessary. Some methods may be abstracted from the practices of other educational campaigns (of any subject-domain) which aim to educate or raise awareness in general society.

Using these premises a number of “trial by error” attempts may be necessary to determine a suitable approach for a societal, cyber-security educational campaign.

The next sections will present a case study of a specific set of such attempts. The next section presents the methodology followed during this study.

3. Methodology

The paper presents a case study (as defined by Creswell (2007)) which spans several years. During these action-research-like cycles of continuous improvement of the process based on lessons learned in previous research cycles is followed. The study follows the case of the annual South African Cyber Security Academic Alliance (SACSAA) educational campaign since 2011. The ultimate aim of the campaign is to foster a cyber security culture via education. This campaign’s target audience is the South African youth. However, the presented results were only successfully gathered and analysed from the youth in the Nelson Mandela Metropolis area.

The campaign itself consists of two parts: an education campaign and a poster contest. The campaign aims to first raise the youth’s awareness of a number of important cyber safety and security topics specific to the practice of cyber security (humans form part of the assets to be protected). These topics cover the issues commonly acknowledged as being relevant to their own cyber activities and existence. The topics covered the following cyber security issues: stranger danger; browsing, downloading and online activities; cyber citizenship; cybercrime; social
networking; cyberbullying; password and hardware security; viruses and malware; cyber –bullying, -harassment and –stalking; cybersex and finally cyber identity management. The contest is secondly used as an instrument to measure the campaign’s impact on the involved youth’s awareness levels. Learners are invited to voluntarily create and submit posters (hand-crafted or digitally-created) which promotes awareness of campaign’s covered security issues.

To aim of this study is to create an educational campaign component which effectively and measurably educates the target audience about cyber issues. The researchers selected three measurements to determine the effective impact of the campaign: learner participation; learner internalization of the lessons; campaign memorability through brand association. The first measurement is self-explanatory. It was measured through the empirical data available in the number of entries. The second measurement of internalization, refers to learning which impacts on knowledge, attitudes and behaviour (KAB). An analysis of the posters and the messages/scenarios they depict indicates how educational lessons was perceived and the degree to which they had been internalized (Van Niekerk et al., 2013). The brand association sought to determine whether the campaign itself as an entity was associated with its message. Inclusion of branding into the posters was an indicator.

This section described how the research has been conducted. The next section will present the overviews, results and analysis of each campaign conducted since 2011.

4. Campaigns and Competitions: Results and Analysis

Each campaign formed an iteration of the research cycle which aimed to improve upon the results of its predecessor. This is attempted through the modification of the existent education campaign based on lessons learned in the previous cycles. This section will discuss the implementation and lessons learned in each year’s campaign.

4.1. Campaign 1 (2011)

The first campaign was run as a voluntary, distance education campaign. It was a “trial run”. The campaign was advertised using professional, promotional flyers. These flyers were distributed via ‘snail mail’ to schools in the Nelson Mandela Metropolis; and posted on the Nelson Mandela Metropolitan University’s campus noticeboards. The pamphlets named topics of interest and encouraged learners to self-study and then participate. Generous cash prizes were offered for the winners.

In total, 3 poster entries were received from NMMU students. Lessons learned were: firstly learners may need to be personally convinced and motivated to become involved. Secondly, to attract school and user attention so as to educate them, a more involved education approach was required. Finally learners may have been more interested in participating if less self-study had been required. Due to the low number of entries no further analysis of the posters was conducted.
4.2. Campaign 2 (2012)

This campaign refocused on solely educating the youth within primary and secondary schools. The invitations were issued via post. Additionally to further attract participants, the researcher personally visited many schools to advertise the campaign and explain its purpose to teachers and learners. The teachers were asked to encourage learner participation in the campaign and competition. Generous prizes were offered for participation in competition.

Several changes were made to the previous campaign approach. To reduce self-study requirements, children were: firstly given a cyber awareness talk by the researcher, and secondly were provided access to relevant material in the form of pamphlets and online topic summary sheets relating to the chosen cyber security issues. Additional resources and reinforcement materials was provided in the format of pedagogically sound games which taught cyber security principles to children through play (Reid and Van Niekerk, 2013). Finally to make the campaign lessons more memorable for the learners, the learners were encouraged to make a cyber safety pledge to themselves and Cyber Sid (a SACSAA partner’s campaign mascot).

This campaign was more successful than its predecessor. A total of 217 poster entries were received. Primary school children accounted for 94 of the entries. The remaining 123 entries were from secondary school children. All of the entries received were from the Nelson Mandela Metropolitan area. This is despite having many requests from schools located all across South Africa for competition flyers, educational material and additional information regarding how to enter. In fact, all entries were received from schools that were personally visited by the researcher. Upon analysis of the posters it was found that 66.18% of all of the participants had (in the researcher’s opinion) successfully internalized the taught messages.

This campaign showed that a more proactive education approach combined with pedagogically-sound supporting educational material and fun activities engaged more participants. The prizes also potentially attracted participants. Additionally it was found that mascots and other branding should be carefully chosen. Several of the children related the mascot to the topic. Many learners included Cyber Sid in their posters. Finally it was found that the teachers in their support role were vital in assisting to promote the campaign to the children. In future campaigns teachers should be asked to participate more actively in the research.

4.3. Campaign 3 (2013)

This campaign implemented almost all of the previous campaign’s procedure. However, a few superficial changes were made. Firstly the Cyber Sid mascot was replaced by the SACSAA logo on all the provided material. Secondly the lectures and support material presented by the researcher was further customised for each school. Upon the teachers’ request particular emphasis was placed on the topic/s which most related to problems learners at that particular school had faced. Cyberbullying was considered a prominent issue by many of the schools. Thirdly
the teachers were provided with access to more support material. They could incorporate these resources into their own classes to reinforce the researcher’s guest lectures. Finally, less generous prizes than previous years were offered.

This campaign was the most successful thus far. In total 468 poster entries were received. Of these entries 275 were from primary school children and 193 were from secondary school children. The analysis of the posters showed that 84.22% of the participants had (in the researcher’s opinion) well internalized the taught messages.

The results of this campaign showed a definite increase in the number of participants. The aggregate of total learners who internalized the message also increased. Unfortunately the number of learners who identified with the mascot/logo decreased.

The analysis of this campaign’s results confirmed most of the previous year’s observation. Firstly it showed that personalization of the material to emphasize each school’s pertinent issues was particularly impactful. For each school that had made a personalization request, the majority of their learners chose that issue as their poster topic. Secondly it showed that increased teacher involvement led to a rise in the percentage of learners who internalized the message. However, this finding is accompanied by a new issue. The level of customization to education material (done by the researcher) cannot be maintained indefinitely using the current educational delivery model. A campaign model which is more scalable is needed.

This section examined the basic results and findings of each year’s campaign. The next section will discuss the aggregate findings in terms of the selected impact measurements described in the methodology.

4.4. Overall Analysis and Discussion (Lessons learned)

The ultimate goal of this research is to determine how to educate society and foster a societal cyber security culture. Thus far this study has shown that the campaign is becoming more effective at achieving this objective for the youth societal sub-group. However, the campaign is not as of yet ideal sustainable, scalable and measurably effective. Furthermore some old and new campaign problems are still being resolved. Some campaign success indicators and problems will now be discussed.

The first indicator of campaign effectiveness is the number of participants each year. Due to the various changes incorporated into the campaign participation has annually increased from 3 entries in 2011 to 463 entries in 2013.

This improvement is encouraging, however, it has resulted in a few new issues being identified. The issue of the limited scalability of the current education campaign model is of particular concern. With the current education model’s delivery methods and degree of customization (done by the research) only a portion of the total target audience is being reached. This is unacceptable therefore a more scalable education delivery model is required to improve the campaigns advancement.
The percentage of learners who internalized the campaign’s lessons are the second indicator of campaign effectiveness. Overall this percentage has increased each year (see Figure 1). The current approach is therefore gaining the learner’s attention and explaining the lessons well enough that the learners are adopting the lessons and considering how the issue affects themselves and others around them.

The third indicator of campaign effectiveness is the campaigns memorability through brand association. This is being established through the use of pedagogy and strategic marketing e.g. the use of a mascot. Thus far, each year the brand association has fluctuated based upon the type of branding logo/mascot used (see Figure 2).

This indicator’s findings show that the selected branding/mascot must be appropriate for the audience. More of the younger children associated with the character mascot than with logo. The older children displayed the opposite tendency. This indicates that to enable a diverse target audience to associate with the campaign, a more flexible but consolidated branding strategy is necessary.

Overall this study has resulted in four principal lessons being learned. Firstly distribution (logistics) definitely impacts how/if the message is received. The current distribution model is not sustainably scalable. Therefore more suitable model should be sought. Secondly teacher involvement is even more crucial than previously supposed. Teacher involvement caused the levels of internalization and participation to increase. If their involvement becomes more focused, the scalability of the campaign could improve. Security experts are capable of communicating the security material however, the results of their methods are not as successful as those obtained when educationalists are involved. Thirdly suitable, official and age appropriate branding is necessary for campaign memorability and relatability. Fourthly the content of the course is well-chosen, however, the presentation and delivery of the course continuously requires improvement. Involvement from appropriate experts should possibly be sought.
4.4.1. Upcoming 2014 campaign (future work)

The will be altered to take into consideration the lessons learned in 2013’s campaign. An attempt to improve the scalability of the campaign by increasing the educational role of the teachers and decreasing the security expert’s presentation role. This year the campaign will follow an adaption of a top-down, organisational culture change approach. Experts will obtain principle top-management support and allow existing hierarchies to further communicate the campaign message. For youth sub-group of society this will be one by getting principal buy in via DOE. Then the security experts will educate the teachers about the campaign topics. The experts will also provide the information about the campaign topics as well as previous campaigns successfully used resources. The researcher will have no contact with the children. The teacher will be expected to customize and present the material to suit their classes and students. Finally lessons learned from this campaign will be used and adapted to guide the development and launch of a parallel campaign which will target another societal subgroup (possibly the organisational sector).
5. Conclusion

The fostering of a societal cyber security culture is vital to educate society about cyber security issues and practices. The lessons learned indicate that to be effective all decisions and implementations of the critical aspects of such a campaign need have a solid theoretical basis. This is particularly important for the selecting and presenting the campaign message.

In this case the most suitable people to ensure that the message is clear is the cyber security subject-domain experts. However, these experts are not necessarily skilled or constantly available enough to any of the other aspects of producing an effective cyber security educational campaign. Therefore the researchers advocate that security expert should determine what to teach users, however, the education and other aspects of the campaign should be done by relevant domain experts. Ultimately the findings or this research strongly suggest that an interdisciplinary approach to education is needed for a cyber-security education needs of a society.

The significance of recognising this need for an interdisciplinary approach could enable the improvement of scalability, quality manageability and continuity possible for a course. Therefore this will aid in developing a culture fostering process which will endure and adapt to change. Further research will focus on developing a framework to enable all involved subject domain specialists to integrate their contributions to create and manage a cyber-security education course which aims to foster a societal cyber security culture.

6. Acknowledgements

The financial assistance of the Vodacom/NMMU and National Research Foundation (NRF) scholarships towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not necessarily to be attributed to the sponsors.

7. References


A Cyber Security Culture Fostering Campaign through the Lens of Active Audience Theory

R. Reid and J. van Niekerk

Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
s208045820@live.nmmu.ac.za, Johan.VanNiekerk@nmmu.ac.za

Abstract

The South African Cyber Security Academic Alliance’s (SACSAA) cyber security educational campaign aims to foster a cyber-safe and -secure culture amongst South Africa’s youth. Previous work shows that the campaign is fostering a cyber security culture amongst its audience. However, it has not determined if the developing culture aligns with the desired cyber security culture that the campaign expected to foster. The target audience’s interpretation of the campaign’s educational messages meanings can affect a developing cyber security culture; possibly resulting in it not aligning with the campaigns preferred culture. This paper examines the audience’s interpretative role in developing a cyber security culture, through the lens of active audience theory. The objective is to enable early detection of deviations between the campaigns objectives and its actual results within the audience.

Keywords

Cyber security culture, cyber security education, Active Audience Theory, Action Research, Case study, SACSAA, Public understanding of security

1. Introduction

In our technology- and information-infused world cyberspace is an integral part of modern-day society. In both personal and professional contexts cyberspace is a highly effective tool in and enabler of most people’s daily digitally-transposed activities (Klimburg 2012; Siponen 2001; De Lange & Von Solms 2012). Several countries governments have recognized the many potential benefits that the adoption of the Internet and ICT may have for their country's welfare (Klimburg 2012). Therefore, in many of these countries, citizens are being actively encouraged to adopt these technologies. The resultant rapid adoption of cyber technologies and services has had some very positive results e.g. providing users access to many beneficial and convenient services and utilities. However, it has also had some negative and often unintended consequences. A prominent, problematic consequence is that the citizens are becoming increasingly technology dependent whilst also becoming increasingly vulnerable to cyber threats (Furnell et al. 2007).

As the number of active cyberspace users increases, so too does the chances of a cyber threat finding a vulnerable target also increase. Most users are not significantly aware of or secured against the cyber threats targeting them. To avoid becoming victims of cyber threats these cyber citizens urgently need to acquire the security- and safety- skills necessary for safe activity within cyberspace (Siponen 2001).
All cyber users who are exposed to the risks and need to be educated about cyber security. However, this education is particularly important for children who interact with cyberspace from an early age (De Lange & Von Solms 2012). A cyber security culture instilled amongst the youth may become an integral part of all their daily activities throughout their increasingly technology infused lifetime. Additionally, these children may further foster the culture by passing it on to their own children in the future. Therefore, it is particularly important that campaigns which target the youth are effective at communicating the right cyber security themed messages. The campaigns should present the messages in a way that enables the children to understand the message as the campaign’s content intends it to be understood.

In South Africa, the South African Cyber Security Academic Alliance (SACSAA) runs an annual campaign which aims to raise school children’s awareness about vital cyber security and safety behaviours. Ideally the campaign aims to aid in the fostering of cyber security culture amongst cyber citizens. This paper asks: “Is the developing cyber security culture, the culture which we intended to foster?”

This paper aims to use active audience theory as a lens to determine whether the SACSAA Cyber Security Campaign’s target audience has been unambiguously and uncritically interpreting the meaning off the educational campaign’s awareness themes (messages) as they were intended to be imposed by the campaign creators. Detecting if the audiences interpretation deviates from the campaign’s intended result may make it easier to identify necessary adjustments for future campaigns.

The remainder of this paper is structured as follows: Section 2 provides more detail about the SACSAA Campaigns. Section 3 provides a preliminary explanation of the active audience theory paradigm. The research design used to meet this papers aim is outlined in Section 4. Section 5 presents the findings of the paper. Finally our work is concluded in Section 6 and limitations of the research are presented in Section 7.

2. The SACSAA Campaign

The South African Cyber Security Academic Alliance (SACSAA) consists of research groups from three well-known South African Universities (SACSAA 2011). The main objective of SACSAA is “to campaign for the effective delivery of Cyber Security Awareness throughout South Africa to all groupings of the population” (SACSAA 2011). Ultimately, SACSAA intends to aid in the fostering of a societal cyber security culture via education. This paper will focus on the data gathered from the SACSAA campaign activities involving the youth. SACSAA has officially run an annual educational cyber security campaign targeting the youth since 2012 (2011 had a pilot study). The campaign consists of two components: an education campaign and a poster contest.

The campaign aims to first raise the youth’s general awareness of the need for cyber security in their digital activities. There are six main thematic messages in the campaign: “Keep your private information private”; “Be nice online”; “Stay legal”; “Trust an adult”; “Protect your PC”; “Stranger Danger”. A wide variety of cyber
security and safety topics within these themes have been covered each year. Mass media is used to distribute messages and cultural forms (information) to large, widely dispersed, heterogeneous audiences (Munday & Chandler 2011). The campaign presents each topics content using multiple mass media modes including: digital media (awareness posters, videos, SACSAA website and online resources), printed media (awareness posters, informational pamphlets, educational games (Reid & Van Niekerk 2013)) and finally public events (interactive school visits).

Each year the campaign has been modified to increase effectiveness of the successive campaign’s results and scalability. Changes and additions to the campaign have included the use of pedagogical theory, use of multimedia and interactive presentations and multimodality in the campaign material, increased contextual customization, increased teacher involvement, inclusion of SACSAA’s branding logos and mascots. Detailed about the modifications and results from 2011 until 2013 are available in previous work (Van Niekerk et al. 2013; Reid & Van Niekerk 2014). In 2014 the campaign was adapted to be more teacher-oriented, and a cyber security school curriculum was provided.

The poster contest is the instrument used to measure the campaign’s effect on the involved youth’s awareness levels. Learners are invited to create and submit a hand-crafted or digital poster showing an awareness message (as they understand it) for one or more of the campaign’s topics. Participation is voluntarily. Evaluations of past campaign iterations competition posters has shown that the majority of participants have internalized (learned from) campaign messages. Posters indicated internalization was: “partial” if the learner depicting the message as it was given; “moderate” if the lesson was rephrased into the learner’s own words; or “full” if the lesson was shown to be contextualized by the learner. It is possible that the raised awareness levels (shown by internalization), and any resultant behaviour modifications could enable the fostering of a culture amongst these participants.

This research aims to determine if the cyber security culture being fostered by the SACSAA campaign aligns with how the culture messages were intended to be being interpreted. The role of the audience in this process has yet to be examined. It is the author’s opinion that active audience theory could be used to understand the role of the campaign’s target audience’s in fostering a cyber security culture. This opinion is due to the campaign’s use of mass media and its purpose of communicating with and having a message understood by an audience (television has the same purpose).

3. **Active Audience theory paradigm**

In cultural studies dealing with television and mass media, understanding the relationship between a media “text” and it’s audience (audience research) (Barker, 2012). In this field, the role of the audience is therefore a research focus. This paper examines the active audience paradigm. Active audience theory examines the active, interpretative role of audience when they “make meaning” from the media content (Hall, 1980; Munday & Chandler, 2011). This paradigm suggests that it should not
be assumed that audiences develop a culture by uncritically accepting the ‘textual’ meaning of a programme (Barker, 2012).

The aim of a media “text” is typically to communicate a message with a specific meaning. The process of communication consists of a circuit of a complex structure of relations namely: production >> circulation >> distribution/consumption >> reproduction of a message (Hall, 1980).

Within this circuit of communication, messages are sent between parties. Typically, the message has a meaning, which the sender tries to convey when constructing and producing the message. However, as the message moves within the circuit, it is not guaranteed that each level interprets the meaning of the message similarly. This is because the meaning of a message is polysemic and an audience is seldomly passive.

The active audience theory paradigm argues media has a preferred message to communicate to their audience, but media audiences do not passively accept information and its imposed meanings from a structured text (Munday & Chandler, 2011). Stuart Hall’s encoding/decoding model (see Figure 1) illustrates this by showing the discourses of the meaning of the text between its producer (encoder) and the reader (encoder) (Hall, 1980).

Within the circuit of communication the encoding/decoding model shows that audiences are active and knowledgeable producers of the meaning a texts delivered message within their personal and social contexts (Barker, 2012). The producer (encoder) encodes meaning in a certain way, while the reader (decoder) decodes it differently according to their own personal knowledge and contextual frames of interpretation. It cannot be assumed that the meaning of a program, text or any other communication has a fixed interpretable meaning, which can unerringly be recognized by any audience. Instead how the audience makes sense of a texts meaning is “the product of a negotiation between the audience and the text in a particular context of reception” (Munday & Chandler, 2011).

In brief, different audiences may accept different textual meanings, based on how the “text” is constructed and communicated. Texts(the messages) are polysemic (can have multiple meanings)(Hall, 1980). Often only some of the meanings will be accepted by an audience (Barker, 2012). The audiences decoding will typically fall into one of the following three hypothetical decoding positions as proposed by Hall:

![Figure 1: Meaningful Discourse (Hall, 1980)](image-url)
• “The dominant-hegemonic encoding/decoding” where the decoder accepts the messages ‘preferred meanings” which a text is attempting to impose (Hall, 1980);
• “A negotiated code” position wherein the decoder acknowledges the legitimacy of the theory of the hegemonic decoding, but adapts it interpretation based on particular circumstances or context (Hall, 1980);
• “An oppositional code were audience members understand the preferred encoding may reject it and decode the text in contrary ways” (Hall, 1980).

All positions are the result of the whole communication process and the decoders (audience) producing their own meaning of the message. For the purposes of this paper, a fourth decoding position could be “null” wherein where the audience members did not understand/accept/ process the message clearly.

Due to the campaigns use of mass media, the authors believe it is possible to apply the encoding/decoding model to the campaign’s audience. The decoding position espoused by the majority of the SACSAA audience’s takes could indicate what type of culture is developing. This could then allow measurement of whether the fostered culture aligns with SACSAA’s intended culture formation.

4. Research design

This research examines a case study of the annual SACSAA educational campaign. This campaign has been running since 2011. Its target audience is the all South African youth. However, thus far data has only been gathered from the numerous schools in the Nelson Mandela Metropolitan area who have been increasingly exposed to the campaign. This paper aims to determine if a culture which has developed over time amongst an audience, matches the campaign’s desired culture. Part of the campaign’s enhancements over the years has been the customization of the material to fit the issues of each particular school. Therefore, in order to measure an effect on an audience and its culture it would be best to examine one particular audience and context i.e. one school which has been exposed to the campaign for several successive years. Therefore, for the purposes of this paper only data gathered from the single school to have participated in every campaign since 2012 until 2014 (last complete campaign) will be used. This school will be referred to as ‘School A’.

‘School A’ is a convenient and purposive sample for the analysis purpose of this paper. Firstly, it is a convenience sample as the data was "available to the researcher by means of its accessibility” (Bryman, 2012). The researchers have been gathering data for a number of successive years for research purposes. Secondly, this sample is also purposive as the sample participants were specifically selected "so that those sampled are relevant to the research questions that are being posed" (Bryman, 2012). Over the years the campaign material and approach has altered and improved. The students within ‘School A’ have been exposed to all of the involved culture fostering and measurement activities. The sample is believed to be representative of the SACSAA campaign’s overall target audience because: the participants are all primary school children; their age ranges between 6 and 15; members of both
genders participated; and different ethnic groups were represented. Due to ethical considerations no identifying data apart from participant age was captured.

A content analysis; as described by Krippendorff (2004); was done to determine if the audiences interpretation of the material aligned with the subject-expert and educator’s intended key messages for each campaign topic. A content analysis can be conducted on texts and artifacts (Hodder, 1994). The researchers consider the SACSAA competition posters to be iconic cultural artifacts, which provide information about the culture of their creators. Therefore the analysis was conducted on the competition posters gathered from ‘School A’. The aim was to determine if the learner’s interpretation and internalization of the educational message matched, closely related (generally agreed with minor differences in interpretation) or opposed the campaign’s intended meanings. For this analysis the following questions were asked for each poster: Firstly, “What topic(s) do the message(s) in the poster cover?” and secondly, “What position within Hall’s encoding/decoding theory did the audience member (poster creator) take once they decoded the campaign’s message (in the researcher’s opinion)?” Each of these questions and the analysis process for answering them will briefly be elaborated upon in the next two subsections.

4.1. Posters per topic

This question was to determine which specific topics were considered more important by the learners. The campaign covered all of its topics well, however, it placed emphasis (considerable content) on the issues it considered critical issues. These thematic issues messages are: promoting anti-cyber-bullying, personal pc and information protection, and staying legal online. The percentage of posters covering a topic will be compared to the ratio of the campaign’s content which covered the topic. The difference between the percentages could indicate a match or difference rating covered issues importance from the audience’s and campaign’s perspective.

4.2. Poster creators decoding position on the related campaign topic’s message (according to Hall’s encoding/decoding theory)

This question was asked to determine if the way the participant interpreted the message of the material aligned with how the campaign intended it to be understood. The participant’s interpretation of the campaign topic(s)’s message(s) (as the show it in their poster) was categorized as having one of the following positions: the dominant-hegemonic decoding position; a negotiated coded position; or an oppositional coded position. These positions meaning according to Stuart Hall are explained in Section 3. In order to determine which of these positions a poster belonged to, the following questions were asked as an evaluation matrix:

- Does the posters textual message support the related campaign topic(s) message?
- Does the posters graphical message (examples/warnings) support the related campaign topic(s) message?
What overall impression (in the researcher’s opinion) does the poster give of the participant’s interpretation of the related campaign topic(s) message?

The answers to these questions were selected to be one of the following: strongly supports related campaign topic’s message; partially/vaguely supports related campaign topic’s message; opposed related campaign topic’s message; undeterminable. If two or more questions were answered as strongly supporting the related campaign topic’s message the poster was classified as having accepted the dominant-hegemonic decoding interpretive position. Likewise, if two or more questions were answered as strongly opposing the related campaign topic’s message the poster was classified as having accepted an oppositional coded interpretive position. Other combinations of answers resulted in the poster being classified as having accepted a negotiated coded interpretive position, unless two or more question was answered as ‘undeterminable’ in which case the posters was classified as having a “null” or “undetermined” position. “Null” position posters were typically considered impossible to interpret without further information. An example of the results of using this matrix may for classification purposes is shown by Figure 2.

Figure 2: Examples of classification of poster interpretaion positions

An example of a poster which is categorised as accepting the dominant-hegemonic (preferred) encoding/decoding of the campaign’s message for the topic of cyberbullying is shown in figure 2a. The text strongly supports prevention and stopping of cyber bullying and provide tips on how to do this. The graphics strongly support the message e.g. it shows the consequences (emotional pain) of the cyber bullying on the victim and the platforms this bullying may occur on. Overall the posters strongly suggests that the participant agrees with the campaigns objective of promoting the prevention of being a cyber-bully and/or victim of cyber bullying. In contrast to figure 2a, figure 2b shows an example of a poster which is categorised as representing an oppositional coded interpretative position for cyber bullying topic. The textual message was classified as being oppositional as it did not discourage cyber bullying in anyway, instead it seemed to say cyberbullying is inevitable and consequences should be disregarded. The graphical pictures illustrated an example of cyber bullying but did not indicate it should be stopped or that it was bad,
therefore they were also classified as being oppositional. Overall the poster seemed to promote cyber-bullying rather discourage it.

The remainder of this paper will discuss the results of the quantitative analysis. It will then conclude with the papers findings in terms of its aim.

5. Analysis and results

This analysis aims to determine if the culture being fostered amongst this audience matches the campaign expected resultant culture. Historically, School A has had 240 learners voluntarily participate in the poster completion (50 learners in 2012, 102 learners in 2013, 90 learners in 2014). Some posters represented multiple themes and topics. The distribution of the posters per campaign topic is shown in figure 3.

Figure 3: Percentage of each year’s posters showing a particular topic

Based on Figure 3, the audience has shown a high rate of acceptance of messages relating to the dangers of interacting with strangers online, keeping their personal information (and passwords) private and secure and prevention of cyber bullying. Contrastingly they do not accept the message of anti-piracy. These four messages were equally focussed on as serious issues in all of the campaign material, as they are issues which are strongly associated to children’s cyber activities. The audience seems to agree with the campaign about the importance personal and asset security and safety; however, they reject the campaign’s view that piracy and infringement of others individuals/entities property rights should be stopped (particularly if they benefit from the infringement). An informal tally done by School A’s teachers found that the majority of the learners had pirated one or more series, film and/or game.

Further analysis evaluated the position of the audiences decoding an interpretation of the campaign topics messages as previously discussed. Figure 4 shows that the majority of learners accepted the campaign’s preferred (dominant-hegemonic) interpretation of message for their chosen topic. Additionally the remainder of the posters positions were categorized as having accepted a negotiated coding position. It is very rare for the posters to be categorized as opposing the message or being undeterminable. This trend is visible in three successive years’ posters.
6. Conclusion

The campaign’s audience has been actively producing meaning from the materials messages. The majority of the audience is decoding the campaign’s messages and accepting the campaign’s preferred message meanings. These findings were particularly strong for messages which strongly related to the participants perceived personal/asset security. However, the findings also indicated that the audience preferred to negotiate or reject messages that they did not perceive to have a negative consequence for themselves e.g. messages relating to piracy. Overall, this paper concludes that the majority of the cyber security culture developing amongst this audience matches the culture which the campaign material aims to foster. This outcome could improve further, if future work establishes how to encode material to encourage audiences to accept the campaign’s less preferred messages.

7. Limitations of this research

Firstly, all conclusions drawn from the qualitative analysis of the posters may be in some measure biased by the researcher’s interpretation of each poster. Secondly, the overall campaign message rejection or negotiation may not be completely measured from the data as learners were only required to include a minimum of one campaign message in their artefact as they understood it.
8. Acknowledgements

The financial assistance of the Vodacom/NMMU and National Research Foundation (NRF) scholarships towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not necessarily to be attributed to the sponsors.

9. References


Appendix C: The human brain and learning
Appendix C

1.1 Introduction

There are currently several conceptual models and theories in both brain- and cognitive-related literature. The brain’s theoretical physio-cognitive ability associations and their involvement in various activities vary from model to model, although the models do also agree on certain issues. However, on a physical level many components from both brain hemispheres are involved in all the activities which a human being performs with both sides of the brain always being involved.

Information flows back and forth physically in a continual cycle between the two hemispheres of the brain (Caine & Caine, 1991; E. P. Jensen, 2008c; Scoffham, 2004). This appendix will examine how this information processing occurs in the human brain, based on a select group of conceptual models which were chosen for their relevancy to the design of the cybersecurity campaign to comply with brain-compatible education (Chapter 6). It explains the neuroscience behind the brain-compatible pedagogy.

1.2 The human brain and learning

Traditionally, both the physical and conceptual representations of the brain describe two linked hemispheres, each which several abilities and activities attributed to it as natural functions (Jensen, 2008a, p. 8). Examples of each hemisphere’s abilities include the different types of information-processing (Gülpinar, 2005).

The left hemisphere of the brain typically operates in a linear, sequential manner using logical, analytical and propositional thought (Gülpinar, 2005). This hemisphere has commonly been associated with activities such as information processing (Scoffham, 2004). Conversely, the right hemisphere of the brain is described as operating in a nonlinear, simultaneous manner, and as dealing with nonverbal information and appositional thought (Gülpinar, 2005). This right side of the brain is present-oriented (Gülpinar, 2005) and is associated with the abilities pertaining to music and spatial awareness (Scoffham, 2004).

The abovementioned brain models are helpful in providing a generalised and basic understanding of the brain and its abilities. However, a more detailed and comprehensive understanding of the
basic biological and cognitive responsibilities of the various areas of the brain is required in order to understand how actual learning takes place.

Physically the brain does, indeed, exist as two connected hemispheres. However, these hemispheres are subdivided into more specialised and specific parts with each part of the brain having a specific agenda and behaving in accordance with this specific agenda (Erlauer, 2003). It is the interplay between the various parts of the brain that results in some of the contradictions and complexities of human behaviour. Paul McLean proposed a three-layered theory termed the “Triune Brain Theory” to explain the functions of these various parts of the brain (Erlauer, 2003; E. P. Jensen, 1995; Scoffham, 2004). The purpose of the proposed layers is to aid in the understanding of the functions and cognitive abilities of the various brain areas. The three layers are categorised as follows, namely, reptilian brain (brain stem), mid-brain (limbic system) and the neo-cortex (upper brain).

The “reptilian brain” or the brain stem, the first layer of the cognitive brain, is located at the base of the brain and is connected to the spinal cord. It is the oldest part of the brain and it produces many of the brain’s chemical messengers. It also controls the automatic, vital functions of the body that ensure the survival of the body, including the heart rate, blood pressure and breathing (Erlauer, 2003). In addition, it is responsible for the motor functions, mating rituals, social hierarchies and role behaviour of the individual (Scoffham, 2004). From a physical-cognitive perspective the brain stem receives messages through the spinal cord from the sensory organs and reacts through the reticular activating system (RAS) (Erlauer, 2003). It filters all the stimuli received, determines their importance and forwards the important stimuli to other parts of the brain for conscious consideration (Erlauer, 2003).

The next layer is the mid-brain or limbic system (Erlauer, 2003; Scoffham, 2004) and is located above the brain stem and the cerebellum. The limbic system regulates our eating, drinking and sleeping habits, as well as our hormones, immune system and emotions (Erlauer, 2003; Scoffham, 2004). In addition, it is the site of long-term memory (Scoffham, 2004). This area leads to an intermediary layer between this second layer of McLean’s model and the final layer, the neo-cortex.

The forebrain is the intermediary layer of the brain which is not part of the “triune” model. It is an area of the brain which consists of the thalamus, hypothalamus, amygdala and cortex. The cortex contains the neo-cortex (Erlauer, 2003). Each brain area plays a specific physical and cognitive role.
The thalamus helps manage the body’s vital functions and transfers some sensory information up to the cortex while the hypothalamus is involved in regulating the normal physical functions of the body (Erlauer, 2003). Together with the amygdala and hypothalamus, the thalamus is also responsible for the fight-or-flight response to danger. The amygdala works with the thalamus to decide which stimuli are dangerous and should be sent to the thinking part of the brain for processing. The hypothalamus is a portion of the brain which is strongly associated with memory. It controls the capture and processing of the immediate memories with its main purpose being to sort what should be acted on or what should sent to long-term memory (Wolfe, 2010). This relates to the third cognitive area of the brain represented in the “Triune” model, namely, the neo-cortex (Erlauer, 2003).

The neo-cortex is the final conceptual layer of the brain in McLean’s model, as explained by Scoffham (2004). This part of the cortex is a complex layer of cells coating the surface of the brain. The neo-cortex is the part of the brain which is strongly associated with cognition and, by implication, learning (Zull, 2006).

The neo-cortex processes the sensory, association and motor functions in different parts of itself (Zull, 2006). Four lobes make up the neo-cortex, namely, the frontal, occipital, temporal and parietal lobes. Each of the lobes has specific functional responsibilities. The frontal lobes are responsible for conscious decision making and are, thus, responsible for all high-level, conscious thinking and sensorimotor planning (Zull, 2006). On the other hand, the occipital lobes are responsible for processing visual information and, as such, they process information about objects, colours, motion and distance, connecting perceived information with past experience and memories to aid the derivation of meaning (Erlauer, 2003; Zull, 2006). The temporal lobes are responsible for processing auditory information and, finally, the parietal lobes are responsible for spatial awareness, processing and analysing sensory stimuli and maintaining the individual’s focus and attention (Erlauer, 2003).

In summary, the neo-cortex is that portion of the brain which is responsible for high-cognitive thought, problem solving, decision making, language, planning, sensory processing, pattern recognition, and reasoning (Erlauer, 2003; Scoffham, 2004). The neo-cortex differs from the lower brain in that some of the neo-cortex’s functions, such as problem solving, involve a conscious effort (Erlauer, 2003; E. Jensen, 1998). It is postulated that it is this portion of the brain which is the most involved in the learning process with this involvement happening at a cellular, or neural, level.
The brain is an organ which comprises a collection of billions of brain cells known as neurons (Erlauer, 2003). The brain’s cortex is organised into several hundred million neural networks or modules (Scoffham, 2004). These modules extend vertically through the cortex in small columns, which are then linked up to form more complex structures. Information is stored in the brain as a result of these neural structures having been established (Abiola & Dhindsa, 2012). “Learning and cognition occurs by establishing of patterns between brain cells” (Scoffham, 2004). This, in turn, implies that, as learning takes place, the brain is stimulated and it changes physiologically.

The brain has the ability to rewire and remap itself as a result of the learning experience. This biological process is known either as “brain plasticity” (Caine & Caine, 1991) or “neuroplasticity” (E. P. Jensen, 2008c). During new experiences and the learning process information is carried inside a neuron by electrical pulses and is transmitted across the synaptic gap between neurons by chemicals termed neurotransmitters (E. P. Jensen, 2008c; McGeehan, 2001; Scoffham, 2004). These electro-chemical pulses, the synaptic leaps of an electrical impulse between the axon of one neuron and the dendrite of another, constitute the physical basis of both learning and memory (Lombardi, 2008; Scoffham, 2004). This process is depicted in figure 1.

![Figure 1 Learning takes place at the synapse (Jensen, 1998b, p. 14)](image-url)
The repeated firing of the newly “fired” cellular pathway causes a chemical change to occur and this, in turn, makes it more likely these pathways will trigger in the future (McGeehan, 2001). This is as a result of the fact that the dendrites of the neuron involved attach to other necessary neurons, thus resulting in a strong neural connection (Abiola & Dhindsa, 2012). This physio-chemical occurrence is known as “Hebbian learning” and represents the physical occurrence of learning in the brain (Erlauer, 2003; Scoffham, 2004). It should be noted that any emotional arousal, either positive or negative, will improve the probability of particular hormones being produced and the protein needed for this reaction to be triggered (Erlauer, 2003). These proteins then settle around the synapse, strengthening the connection. This process is the goal of the brain-compatible education techniques which will be discussed later. The resultant cellular changes constitute the biological form of knowledge (Zull, 2006).

In short, what occurs during the learning process is an actual physical change termed “nerve branching” (E. P. Jensen, 2008b). This branching produces a thicker cerebral cortex and, consequently, more neural connections (see figure 2). It is as a result of the availability of a multitude of available connections between neurons that the processing, retrieval and storing of information becomes easier. In addition, because neurons are highly correlated with memory, mood and learning (E. P. Jensen, 2008b), neurons and neural networks orchestrate a response in the area of learning, education and cognition (Lopez & Alipoon, 2000).

Figure 2 How neurons make connections. Axon-synapse-dendrite pathways are electrical to chemical to electrical (Jensen, 1998b, p. 12)
Irrespective of a person’s age, sex, nationality or cultural background, each individual’s brain has the ability to detect patterns and approximations, and to self-correct and learn from experience. This happens through the analysis of external data, self-reflection and an inexhaustible capacity to create and demonstrate creative thought (Caine & Caine, 1991). In addition, every individual’s brain has the capacity for numerous types of memory. However, the use of, skill in the use of and preferences for a specific type of or combination of memory types is unique to each individual (Caine & Caine, 1990). The reason for this is that the brain’s systems and abilities all integrate differently in the case of every individual as a result of the fact that the brain structure of each individual changes as information is interpreted while the learning process which occurs each individual’s brain becomes more unique (Caine & Caine, 1990).

Throughout an individual’s lifetime, the brain performs constant self-adjustment and self-optimisation processes on itself, resulting in a unique brain structure specific to the individual concerned. The purpose of this constant reconstruction is to help the individual to cope with the ongoing changes in and demands of their cognitive, behavioural and emotional status (Gülpinar, 2005). Ultimately, this demonstrates that the brain has a phenomenal capacity for change and it is possible for learning to utilise this capacity for change (Abiola & Dhindsa, 2012).

Knowing how the brain works in relation to memory and learning is the first step in devising an effective education solution. Most educators are determined to try to enhance the learner’s ability to learn. This includes committing knowledge and skills to memory, retrieving the same knowledge and skills and demonstrating that he/she has learnt the knowledge and skills (Banikowski, 1999).

The relation between brain systems and complex cognition and behaviour, can only be explained satisfactorily by a comprehensive blend of theories and facts related to all the levels of organization of the nervous system, from molecules, and cells and circuits, to large-scale systems and physical and social environments … We must beware of explanations that rely on data from one single level, whatever the level may be (Antonio Damasio as cited by Jensen, 2008b, pg 3).

Strategies and techniques that enhance both memory and the learning process are required to facilitate a variety of learning goals. It is essential that these techniques facilitate the gaining of a learner’s attention and engagement in the lesson, activate prior knowledge and experiences, facilitate the ability to construct meaning and, finally, enable the learner to demonstrate the results of his/her learning. Brain-compatible education is the "engagement of strategies based on principles derived from an understanding of the brain" (E. P. Jensen, 2008a).
1.3 Conclusion

This appendix provided a brief explanation of the physical neurological processes which occur within the brain during learning experiences. These processes form the basis on which brain-compatible education principles are founded. The brain compatible pedagogy and its principles themselves, are discussed in section 5.2.

References


Appendix D: Chapter 6 Figures and Tables
Appendix D
This appendix presents additional figures and tables for Chapter 6.

1. Figures and Tables

Figure 1 2012 SACSAA campaign and poster competition advertisement
Figure 2 2013 SACSAA campaign and poster competition advertisement
Table 1 Consolidated results of each schools’ learners who answered each assessment's questions correct

<table>
<thead>
<tr>
<th></th>
<th>Question 1</th>
<th>Question 2</th>
<th>Question 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Pre-play Assessment</td>
<td>Post-play Assessment</td>
<td>Follow-up Assessment</td>
</tr>
<tr>
<td>All Schools</td>
<td>57.14 94.29 97.14</td>
<td>31.43 77.14 91.43</td>
<td>62.86 91.43 97.14</td>
</tr>
<tr>
<td>School A</td>
<td>54.55 90.91 100.00</td>
<td>45.45 72.73 90.91</td>
<td>63.64 81.82 100.00</td>
</tr>
<tr>
<td>School B</td>
<td>66.67 100.00 100.00</td>
<td>22.22 88.89 100.00</td>
<td>55.56 100.00 100.00</td>
</tr>
<tr>
<td>School D</td>
<td>53.33 93.33 93.33</td>
<td>26.67 73.33 86.67</td>
<td>66.67 93.33 93.33</td>
</tr>
</tbody>
</table>
ENTER THE

2014 Cyber Security Poster Contest
17 October - 21 November 2014

What’s it all about?
The South African Cyber Security Academic Alliance (SACSAA) is seeking creative and educational posters on cyber security topics to be used in cyber awareness campaigns.

Why should you enter?
If your poster is selected, your work might get exposure on:
- SACSAA website
- SACSAA calendar
- School and campus security awareness campaigns
- Media announcements

Submission of entries
Deadline to enter: 21 November 2014

PRIZES
Awesome prizes to be won!
Winners will be announced on 27 November 2014
Prizes to be handed out at a prizegiving ceremony.

Want more information?
For additional material or more information, please contact us at:
E-mail: contest@cyberaware.org.za
www.cyberaware.org.za/contest

Categories
- Cyberbullying
- Cybercrime
- Online Activity Dangers
- Cyber Citizenship
- Stranger Danger
- Protecting Your PC
- Cyber Sexting
- Social Networking
- Browsing & Downloading
- Cyber Identity
- Malware & Software Protection
- Viruses
- Cyber Management

Figure 3 2014 SACSAA campaign and poster competition advertisement
Figure 4 2015 SACSAA campaign and poster competition advertisement
Table 2 Percentage of School A's posters per AAT encoding/decoding position for each topic: Cycle 1 - Cycle 4

<table>
<thead>
<tr>
<th>Topic</th>
<th>Dominant-hegemonic Decoding</th>
<th>Negotiated Decoding</th>
<th>Oppositional Decoding</th>
<th>&quot;Null&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stranger Danger</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cycle 1</td>
<td>84.21</td>
<td>10.53</td>
<td>2.63</td>
<td>2.63</td>
</tr>
<tr>
<td>Cycle 2</td>
<td>64.71</td>
<td>23.53</td>
<td>0.00</td>
<td>11.76</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>53.33</td>
<td>40.00</td>
<td>6.67</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>78.57</td>
<td>7.14</td>
<td>0.00</td>
<td>14.29</td>
</tr>
<tr>
<td>Social Networking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cycle 1</td>
<td>100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 2</td>
<td>80.00</td>
<td>20.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>80.00</td>
<td>20.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>85.71</td>
<td>14.29</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Browsing and Downloading</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cycle 1</td>
<td>100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 2</td>
<td>75.00</td>
<td>0.00</td>
<td>25.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>85.71</td>
<td>14.29</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Dangers of Online Activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cycle 1</td>
<td>90.00</td>
<td>10.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 2</td>
<td>100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>0.00</td>
<td>66.67</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>66.67</td>
<td>33.33</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cyberbullying</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cycle 1</td>
<td>50.00</td>
<td>33.33</td>
<td>0.00</td>
<td>16.67</td>
</tr>
<tr>
<td>Cycle 2</td>
<td>66.67</td>
<td>22.22</td>
<td>0.00</td>
<td>11.11</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>68.00</td>
<td>30.00</td>
<td>2.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>78.57</td>
<td>7.14</td>
<td>7.14</td>
<td>7.14</td>
</tr>
<tr>
<td>Cyber Citizenship</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cycle 1</td>
<td>100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 2</td>
<td>100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>66.67</td>
<td>33.33</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>33.33</td>
<td>16.67</td>
<td>0.00</td>
<td>50.00</td>
</tr>
<tr>
<td>Cyber Crime</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cycle 1</td>
<td>50.00</td>
<td>50.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 2</td>
<td>100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>50.00</td>
<td>50.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>85.71</td>
<td>14.29</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Dominant-</td>
<td>Negotiated</td>
<td>Oppositional</td>
<td>Undeterminable</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>------------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td>hegemonic</td>
<td>Decoding</td>
<td>Decoding</td>
<td>&quot;Null&quot;</td>
</tr>
<tr>
<td>Information and Password Security</td>
<td>Cycle 1</td>
<td>82.61</td>
<td>4.35</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 2</td>
<td>80.00</td>
<td>13.33</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3</td>
<td>87.50</td>
<td>12.50</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4</td>
<td>80.56</td>
<td>5.56</td>
<td>5.56</td>
</tr>
<tr>
<td>Hardware Security</td>
<td>Cycle 1</td>
<td>20.00</td>
<td>40.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 2</td>
<td>50.00</td>
<td>50.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3</td>
<td>77.78</td>
<td>22.22</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4</td>
<td>75.00</td>
<td>8.33</td>
<td>0.00</td>
</tr>
<tr>
<td>Viruses and malware</td>
<td>Cycle 1</td>
<td>75.00</td>
<td>25.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 2</td>
<td>68.42</td>
<td>26.32</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3</td>
<td>42.86</td>
<td>42.86</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4</td>
<td>72.73</td>
<td>9.09</td>
<td>9.09</td>
</tr>
<tr>
<td>Piracy</td>
<td>Cycle 1</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 2</td>
<td>0.00</td>
<td>0.00</td>
<td>100.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3</td>
<td>100.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>
Table 3 Percentage of School D’s posters per AAT encoding/decoding position for each topic: Cycle 2 - Cycle 4

<table>
<thead>
<tr>
<th>Topic</th>
<th>Dominant-hegemonic Decoding</th>
<th>Negotiated Decoding</th>
<th>Oppositional Decoding</th>
<th>Undeterminable &quot;Null&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stranger</td>
<td>Cycle 2 77.78</td>
<td>22.22</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Danger</td>
<td>Cycle 3 29.23</td>
<td>1.54</td>
<td>0.00</td>
<td>1.54</td>
</tr>
<tr>
<td></td>
<td>Cycle 4 70.00</td>
<td>30.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Social Networking</td>
<td>Cycle 2 100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3 24.62</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4 83.33</td>
<td>16.67</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Browsing and Downloading</td>
<td>Cycle 2 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3 1.54</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4 25.00</td>
<td>75.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Dangers of Online Activities</td>
<td>Cycle 2 100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3 7.69</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4 83.33</td>
<td>0.00</td>
<td>0.00</td>
<td>16.67</td>
</tr>
<tr>
<td>Cyberbullying</td>
<td>Cycle 2 69.77</td>
<td>9.30</td>
<td>18.60</td>
<td>2.33</td>
</tr>
<tr>
<td></td>
<td>Cycle 3 18.46</td>
<td>7.69</td>
<td>6.15</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4 72.41</td>
<td>17.24</td>
<td>3.45</td>
<td>6.90</td>
</tr>
<tr>
<td>Cyber Citizenship</td>
<td>Cycle 2 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3 3.08</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4 100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cyber Crime</td>
<td>Cycle 2 100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Information and Password</td>
<td>Cycle 2 80.00</td>
<td>20.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3 40.00</td>
<td>9.23</td>
<td>1.54</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4 92.00</td>
<td>4.00</td>
<td>4.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Hardware Security</td>
<td>Cycle 2 100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3 1.54</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>
### Table 3 continued.

<table>
<thead>
<tr>
<th></th>
<th>Dominant-hegemonic Decoding</th>
<th>Negotiated Decoding</th>
<th>Oppositional Decoding</th>
<th>Undeterminable &quot;Null&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Viruses and malware</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cycle 2</td>
<td>100.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>0.00</td>
<td>1.54</td>
<td>1.54</td>
<td>1.54</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>0.00</td>
<td>100.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td><strong>Piracy</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cycle 2</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 3</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Cycle 4</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Topic</td>
<td>Cycle 3</td>
<td>Cycle 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------</td>
<td>---------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Stranger Danger</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant-hegemonic Decoding</td>
<td>40.00</td>
<td>20.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated Decoding</td>
<td>20.00</td>
<td>20.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppositional Decoding</td>
<td>20.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undeterminable &quot;Null&quot;</td>
<td>20.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Social Networking</strong></td>
<td>92.86</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant-hegemonic Decoding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppositional Decoding</td>
<td>0.00</td>
<td>7.14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undeterminable &quot;Null&quot;</td>
<td>0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Browsing and Downloading</strong></td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant-hegemonic Decoding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppositional Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undeterminable &quot;Null&quot;</td>
<td>0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dangers of Online Activities</strong></td>
<td>100.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant-hegemonic Decoding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppositional Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undeterminable &quot;Null&quot;</td>
<td>0.00</td>
<td>11.11</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cyberbullying</strong></td>
<td>88.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant-hegemonic Decoding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated Decoding</td>
<td>0.00</td>
<td>4.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppositional Decoding</td>
<td>0.00</td>
<td>8.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cyber Citizenship</strong></td>
<td>75.00</td>
<td>25.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant-hegemonic Decoding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated Decoding</td>
<td>9.68</td>
<td>9.68</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppositional Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undeterminable &quot;Null&quot;</td>
<td>0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cyber Crime</strong></td>
<td>50.00</td>
<td>50.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant-hegemonic Decoding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppositional Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undeterminable &quot;Null&quot;</td>
<td>0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Information and Password Security</strong></td>
<td>85.71</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant-hegemonic Decoding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated Decoding</td>
<td>14.29</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppositional Decoding</td>
<td>0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undeterminable &quot;Null&quot;</td>
<td>7.69</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hardware Security</strong></td>
<td>50.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant-hegemonic Decoding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppositional Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Viruses and malware</strong></td>
<td>100.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant-hegemonic Decoding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppositional Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undeterminable &quot;Null&quot;</td>
<td>0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Piracy</strong></td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominant-hegemonic Decoding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negotiated Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oppositional Decoding</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undeterminable &quot;Null&quot;</td>
<td>0.00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topic</td>
<td>Cycle 1</td>
<td>Cycle 2</td>
<td>Cycle 3</td>
<td>Cycle 4</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Stranger Danger</td>
<td>88.00</td>
<td>75.71</td>
<td>73.21</td>
<td>74.36</td>
</tr>
<tr>
<td>Social Networking</td>
<td>97.14</td>
<td>127.59</td>
<td>89.36</td>
<td>84.62</td>
</tr>
<tr>
<td>Browsing and Downloading</td>
<td>100.00</td>
<td>75.00</td>
<td>100.00</td>
<td>63.64</td>
</tr>
<tr>
<td>Dangers of Online Activities</td>
<td>90.00</td>
<td>87.18</td>
<td>75.00</td>
<td>72.22</td>
</tr>
<tr>
<td>Cyberbullying</td>
<td>84.15</td>
<td>109.48</td>
<td>70.86</td>
<td>77.05</td>
</tr>
<tr>
<td>Cyber Citizenship</td>
<td>100.00</td>
<td>77.78</td>
<td>76.92</td>
<td>66.67</td>
</tr>
<tr>
<td>Cyber Crime</td>
<td>85.71</td>
<td>112.50</td>
<td>50.00</td>
<td>90.00</td>
</tr>
</tbody>
</table>
Table 3 continued.

<table>
<thead>
<tr>
<th>Dominant-hegemonic Decoding</th>
<th>Negotiated Decoding</th>
<th>Oppositional Decoding</th>
<th>Undeterminable &quot;Null&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information and Password Security</strong></td>
<td>Cycle 1</td>
<td>88.00</td>
<td>4.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 2</td>
<td>92.66</td>
<td>11.93</td>
</tr>
<tr>
<td></td>
<td>Cycle 3</td>
<td>85.11</td>
<td>12.77</td>
</tr>
<tr>
<td></td>
<td>Cycle 4</td>
<td>85.33</td>
<td>5.33</td>
</tr>
<tr>
<td><strong>Hardware Security</strong></td>
<td>Cycle 1</td>
<td>20.00</td>
<td>40.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 2</td>
<td>66.67</td>
<td>33.33</td>
</tr>
<tr>
<td></td>
<td>Cycle 3</td>
<td>82.35</td>
<td>17.65</td>
</tr>
<tr>
<td></td>
<td>Cycle 4</td>
<td>75.00</td>
<td>8.33</td>
</tr>
<tr>
<td><strong>Viruses and malware</strong></td>
<td>Cycle 1</td>
<td>88.89</td>
<td>11.11</td>
</tr>
<tr>
<td></td>
<td>Cycle 2</td>
<td>90.63</td>
<td>15.63</td>
</tr>
<tr>
<td></td>
<td>Cycle 3</td>
<td>50.00</td>
<td>40.91</td>
</tr>
<tr>
<td></td>
<td>Cycle 4</td>
<td>57.89</td>
<td>21.05</td>
</tr>
<tr>
<td><strong>Piracy</strong></td>
<td>Cycle 1</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 2</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 3</td>
<td>100.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Cycle 4</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>
Appendix E: Snakes and Ladders Instruments
Appendix E

1. Introduction

This appendix introduces the instruments used to gather the quantitative and qualitative data to evaluate the effectiveness of the use of a pedagogically sound cybersecurity game, as an educational tool.

The use of educational games, as well as compliance with a pedagogy, are both recommendations of information-security educational literature. However, the use of pedagogically designed games to educate school learners about cybersecurity is seldom reported on. During the action-research process, a pedagogically designed cybersecurity game was introduced.

Cycle 1 (section 6.3.2) of the action-research process introduced a cybersecurity relevant version of the children’s game *Snakes and Ladders*, as an educational tool (section 6.3.2.2.2). The games were designed to comply with pedagogical principles and to teach various cybersecurity topics. The game’s design complies with the principles of brain-compatible pedagogy. Variations of the game present the content of several cyber-security topics. The specific game board of interest from the section 6.3.2.2.2 description and subsequent evaluation was the password given to the management board.

The educational cybersecurity game was intended for use as an instructive tool. However, the effectiveness of the game as an educational tool had yet to been measured. Use of the game would only have educational benefits; if it had an effect on the learner’s subject-relevant knowledge. Measuring the effect of the game on a learner after a learning experience was, consequently a necessity.

Measuring the effect or success of the game is not only necessary from the viewpoint of evaluating the game. In any learning experience it is also necessary to establish whether learning has taken place. In formal education a re-enforcement activity or assessment typically follows the introduction of newly taught concepts. Teachers expect the components of an educational experience to include objectives, educational resources, procedures, as well as assessments.

A decision was taken to measure the game’s effect on the learners’ knowledge; and thereby to evaluate the games' usefulness or effectiveness as an educational tool. In order to take advantage of the school environment in which the game was played, a plan was formulated to
unobtrusively measure the games’ effect, as part of the educational experience. The method used to measure the games’ effect would also be an assessment tool within the educational experience. The inclusion of an assessment would align with the learners' and teachers’ expectations of most educational experiences.

Due to the vulnerable nature of the target audience, the researcher did not directly interact with the students. All assessments and interactions were undertaken by the participating teachers, as part of their usual class routine. Following the provided procedures, the teachers incorporated the informal and fun game-play lessons, as well as their related assessment into their lesson plans. During these sessions, the teachers made use of the provided educational and assessment tools to obtain the measurements necessary for the evaluation.

In order to measure the effect that the game has on the learners, several measurements are required. These measurements would include:

1. The learner’s initial subject-relevant knowledge and awareness level.

   This measurement measures the learner’s initial knowledge and awareness of the topic that the game has presented. The purpose of this measurement is to establish the baseline awareness level; so that future measurements could be compared therewith.

2. The learner’s subject-relevant knowledge and awareness – immediately after playing the game.

   The second measurement required is that of the learner's awareness levels in relation to the games’ topic – immediately after playing the game. This measurement enables the researchers and the teacher to determine whether the learners could recall the lessons taught by the game immediately after playing it. This measurement assists in determining whether the game was successful, as being educational in the short term.

3. The learner’s long-term subject-relevant knowledge and awareness, after playing the game.

   The third measurement is of the learner’s awareness levels in relation to the game’s topic after a long period of time. This measurement should assist in determining whether the learners can still recall the lessons learnt via the game after a long period of time, without any further exposure to it. The ability to recall the lessons, would indicate that the game had a long-term impact on the learner’s awareness levels. For research purposes, teachers who had agreed to submit the results of the assessments to researchers for
use in evaluating the effect of the game, would be asked to not allow learners to replay the game between the original and follow-up sessions. Additionally, it would be requested that the involved learners also not be exposed to any other topic-relevant material. This would ensure that the measurement was a true measurement of the games effectiveness.

4. The teacher’s perceptions of the effect that the games had on the learner’s knowledge and behaviour.

The final measurement was to record the perceptions of the learner’s teachers on the effectiveness of the game. The teachers would be best suited for monitoring and making observations about the learner’s awareness and behaviour in relation to the games’ topic.

In order to gather the above measurements, it would be necessary to conduct multiple assessments. An initial assessment would be required before the learners were exposed to the game. A second assessment would be required after the game had been played. A third and final assessment would be required, after an extended period of time – after the educational experience, which made use of the game. The assessment tools required within each of these assessment phases will be presented in the next section.

2. Assessment tools

In order to assess the learner’s knowledge, questions (quiz questions) that related to the games’ lessons would need to be asked. These questions would assist in determining what the learner did or did not know. To assess knowledge changes in relation to specific content or lessons, a variety of questions, which deal with the content, would need to be asked at different times.

Three versions of the assessment questions are required for teachers to use in their assessments. The questions should deal with the same lessons, but be presented differently. Each set of questions is for use at different stages of the evaluation. There are sets of questions for the pre-play, post-play and follow-up assessment phases.

In the evaluation of the password-management game, the questions will deal with the following three lessons taught by the board:

1. Never write your password down.
2. Trust your parent or guardian with our password.
3. Use special characters and numbers to make your password, rather than easily guessed information.

The teachers were required to use the questions sets in the order and phases they are presented in below. However, within each informal assessment, the teachers were allowed to ask and discuss the questions, in an order of their own choosing. The teachers recorded a tally of students who selected each answer for each question. These tallies provided quantitative data for analysis.

The questions all asked the same content, and had the same correct answers; however, they were rephrased and re-ordered. The forthcoming sections will present the different versions of the informal assessment.

2.1. Pre-play Assessment Questions

This section presents the first version of the questions, which the teachers could use to assess the learner’s knowledge of password-security practices. These questions were included to measure the initial knowledge of the subject domain (the first measurement). Therefore, these questions were asked before the learners had played the game for the very first time.

Three questions, which related to the lessons taught by the board, were asked. These questions, and their potential answers, are:

1. Where should you write down your password?
   A. On a piece of paper
   B. Nowhere
   C. In a book

2. Who may you share your password with?
   A. Your mom and/or dad
   B. Your best friend
   C. Someone who shares their password word with you
   D. Anyone who asks for it

3. What should you use to make your password?
   A. Your pet’s name
   B. Special letters and numbers
   C. A word from a dictionary
The correct answers were as follows: question 1 (Option B), question 2 (Option A) and question 3 (option B).

### 2.2. Post-play Assessment Questions

This section presents the second version of the questions, which the teachers could use to assess the learner’s knowledge of password security after the learners had played the game. These questions addressed the same lessons related to the pre-play assessment questions; however, they had been rephrased, or they had replaced any incorrect answers. The questions aimed to determine whether the game had an immediate effect on the learner’s knowledge (the second measurement). The altered version of the three questions, and their potential answers, are:

1. Where should you write down your password?
   - A. Nowhere
   - B. On a list
   - C. In your diary

2. Lots of people can ask for your password. Who should you tell it to?
   - A. Your online friends
   - B. Your mom and/or dad
   - C. Your best Friend
   - D. People that ask for it

3. What should you use to make a strong password that you can remember?
   - A. Your address
   - B. Big and small letters, numbers and symbols
   - C. Your mom’s name

The correct answers were as follows: question 1 (Option A), question 2 (Option B) and question 3 (option B).

### 2.3. Follow-up Assessment Questions

This section presents the third and final version of the questions, which the teachers could use to assess the learner’s knowledge of password security. These questions were to be asked after the game had not been played for an extended period of time. These questions addressed the same lessons related to the pre-play and post-play assessment questions; however, they had been rephrased or had the incorrect answers replaced. The questions aimed to determine whether the game had a long-lasting impact on the learner’s subject-relevant knowledge and
awareness levels (the third measurement). The final version of the questions, and their potential answers, are:

1. Where should you write down your password to keep it safe?
   A. Nowhere
   B. In a book
   C. On a list of passwords
2. Who should you trust with your password?
   A. Your mom and/or dad
   B. Your best Friend
   C. Someone who shares their password worth you
   D. Anyone who asks for it
3. What can be used to make a strong password?
   A. Your telephone number
   B. A difficult word from a dictionary
   C. Numbers, symbols and letters from the alphabet

The correct answers were as follows: Question 1 (Option A); question 2 (Option A); and question 3 (option C). Following the final informal assessment session, the researchers also spoke with the teachers to hear their perceptions of the games’ affect.

The assessments were planned to provide teachers and the researchers with the opportunity to assess whether the game had impacted the learners’ relevant knowledge. The teachers could use the assessment to provide feedback to the learners; and they could take into consideration what was learnt and what needs to be re-inforced when planning future lessons. The researchers could use the data gathered from the assessments to evaluate the overall effectiveness of the game – as an educational tool to be included in the campaign effort. Additional data, which could assist the researchers in their evaluation of the effectiveness of the game, would be the observation of any relevant behavioural changes learners may exhibit after playing the game, and the opinions of the teachers who implemented the game play.

The next section will discuss how these further data were acquired.

3. Informal open-ended interviews

The fourth and final measurement required to evaluate the effectiveness of using an educational cybersecurity game, which complied with the pedagogical principles was the teacher’s
perceptions of the games’ effect on the learners. The teachers who conducted the play sessions and informal assessment session were in a position to observe learner’s behaviour before, during and after playing the cybersecurity game. Thus, they could monitor and comment on any behavioural changes, which could have occurred.

The researchers held individual, informal feedback sessions with the teachers, who were involved in the research process for evaluating the game and its effectiveness as a cybersecurity educational tool. The feedback sessions involved open-ended discussions, which allowed the teachers to provide any and all feedback that they felt was relevant to the games impact on the learner’s knowledge and behaviour.

These discussions yielded qualitative data to be used in the overall evaluation of the games’ effectiveness.

**4. Conclusion**

The assessments the teachers conducted with the learners; and the informal open-ended discussions between the researcher and the teachers yielded quantitative and qualitative data. These data could be used to evaluate the effectiveness of the compatible cybersecurity Snakes and Ladders board game. This appendix presented the description of the instruments used to conduct these assessments.

The implementation of the assessments is described in section 6.4.2.3 and section 6.4.3.3. The results of the assessments and the discussions are presented in section 6.4.2.4.1 and section 6.4.3.4.2.
Appendix F: Cybersecurity and Cybersafety Curriculum
Dear Teacher

Cyberspace has brought many advantages to all of us. Most of us, learners, teachers and parents, have grown almost totally dependent on cyberspace for our everyday recreation, social networking, communication, etc. We can hardly imagine a day without cell phones, the Internet, Google, Facebook, YouTube and many more Internet and cyber-based services.

Unfortunately, along with all of these advantages in cyberspace came a whole series of cyber related risks. Sharing too much private information, cyber bullying, exposure to paedophiles, sexting, losing money are merely a few of these modern-day cyber-related risks we need to contend with and educate our children about.

The Group for Research in Information and Cyber Security (GRICS) at the NMMU has developed a curriculum to teach cyber safety to learners in Primary Schools. The goal of this curriculum for teaching cyber safety is basically twofold;

i. to empower teachers at primary schools to offer such cyber safety lessons and

ii. to educate learners of age groups 10 to about 14 the basic principles of cyber safety relevant to their typical activities in cyberspace.

To offer this curriculum, the following need to be noted:

i. The material will provide introductory information to the teacher to present suitable content to learners and facilitate discussion afterwards on a specific cyber safety topic.

ii. The curriculum is divided into two age groups; ages 10 - 12 and 13 and older respectively. For each age group a number of lessons on specific topics are prepared. Some of these lessons may overlap to some extent to reiterate some aspects.

iii. Each lesson is made-up of three pages. Page 1 is a lesson plan for the teacher, page 2 an assessment exercise for the learners and page 3 a memorandum of the exercise. Ideally teachers should print and duplicate the assessment exercise for the learners to complete after they watched the video and discussed the lesson.

iv. To offer the content, a school does require a computer that is linked to an Internet connection and ideally a data projector with audio.

v. The intellectual property (IP) of this curriculum belongs to the NMMU.

The curriculum is making it easy for teachers to present, discuss and assess various aspects of cyber safety with their learners in class or in an IT laboratory. The teachers will also be educated to some degree in the process to be able to assist learners with cyber safety issues and problems like; cyber bullying, sexting, etc.

Although this material is the property of the Nelson Mandela Metropolitan University, please feel free to use, copy and distribute the material to interested parties.

Rossouw von Solms (Prof)
Table of Contents

Age: 10 – 12 years
Lesson 1- Phishing attacks and Viruses
Lesson 2- Web Information
Lesson 3- Sharing personal information
Lesson 4- Cyber Bullying
Lesson 5- Summary of SMART lessons
Lesson 6- Password protection
Lesson 7- Viruses and Antivirus Software
Lesson 8- Accepting friend requests
Lesson 9- Privacy Settings
Lesson 10- Cyber Bullying
Lesson 11- Meeting online friends in real life
Lesson 12- Online Game Addiction
Lesson 13- Illegal Downloads
Lesson 14- Cyber Bullying

Age: 13 – 15 years
Lesson 15- Online privacy
Lesson 16- Cyber Bullying
Lesson 17- Share with care
Lesson 18- Online safety
Lesson 19- Safe social networking
Lesson 20- Cyber privacy
Lesson 21- Cyber Bullying
Lesson 22- Online posting can haunt you in the future
Lesson 23- Be careful of online friends
Lesson 24- Sexting
Lesson 1:
Phishing attacks and Viruses

Overview:
Cyber safety refers to the technologies and processes designed to protect computers, networks and data from unauthorised access, vulnerabilities and attacks delivered via the Internet by cyber criminals. Cyber safety threats include viruses, spyware and worms among many others and can severely compromise computer systems and networks.

In this first cyber safety lesson, we handle the topic of phishing and viruses. Phishing is the attempt to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity through electronic communication. An example includes disguising an email to be from a bank asking for log in details where the user does not know the email is illegitimate. Viruses are malicious programs which intention is to harm a computer system. Viruses are transferred between computer systems over the Internet, through emails and using portable storage such as USB drives.

Learning Objectives:
Primary:
1. Know what cyber safety is in general.
2. Understand viruses and phishing as cyber safety threats.

Secondary:
1. Be able to identify a possible phishing threat.
2. Know how viruses are distributed and how to protect yourself against it.

Materials:
Video: The adventures of Kara, Winston and the smart crew, Chapter 1
http://www.youtube.com/watch?v=svb6d55e29k

Procedure:
1. Introduce the general concept of cyber safety.
2. Watch video.
3. Reflect on video with class discussion.
4. Explain main lesson concepts.
5. Do class assessment to measure understanding and insight.

Discussion:
Questions for class discussion:
1. What do you think is a virus?
2. Can anyone tell me what phishing is? (Compare with fishing)
3. Why did Cookie yell “Danger!” when Winston received the email?
4. How can you identify a dangerous email?
5. Can you give your names and passwords to friends you meet online?
6. What are some of the advice given by the smart crew?
7. Does anyone know how you can protect yourself from viruses?

Assessment:
Fill in missing words and complete the word search assignment.
Lesson 1: Assessment

Instruction: Fill in the missing words in the following sentences. Upon completion, find the words in the word search. Make sure you find all of the words.

Questions:
1. Our friends on the pirate ship are _________, ___________ and ___________ the monkey.
2. When they want to get advice on suspicious activities, our pirate friends consult the _________ crew for help.
3. The crew’s computer would have been infected with a _________ if they opened the _________ that was sent with the email.
4. ___________ is when someone makes you think they are your friend and asks for your personal details, but they are actually a cyber crook disguising himself as your friend.
5. I can protect my computer against viruses by using an ___________ program.
6. Never trust an ___________ from someone you don’t know.
7. A is for ___________.

Words:

SICKNESS - ANTIVIRUS - PHISHING - VIRUS - COOKIE - ATTACHMENT - ACCEPTING - KARA - SMART - WINSTON - EMAIL - ADVICE BLACKOWL - MESSAGE

Word Search:

M F O T E S G T O S U R I V Y
L E W E L W O K C A L B J Q U
W S S P I P J A Z A Y G C D K
R T X H A K L O Z J C J A N T
Q F E H R D O Q P N N N N T W
F W J W A Y V O Z M O U T K O
Z C D V K U M I C A T E I N L
J B E S S E N K C I S D V T H
K K P X S A J C Y E N V I O K
E H R S L Y E B O S I A R O Y
J Z A I R P A M M K W X U O M
Y G A B T Y Q A I J V M S H I
E M T I S V R O L B V M W O U
E Q N Y V T N E M H C A T T A
O G E P H I S H I N G J L U N
Lesson 1: Memorandum

Instruction: Fill in the missing words in the following sentences. Upon completion, find the words in the word search. Make sure you find all of the words.

Questions:

1. Our friends on the pirate ship are Kara, Winston and Cookie the monkey.
2. When they want to get advice on suspicious activities, our pirate friends consult the smart crew for help.
3. The crew’s computer would have been infected with a virus if they opened the attachment that was sent with the email.
4. Phishing is when someone makes you think they are your friend and asks for your personal details but they are actually a cyber-crook disguising himself as your friend.
5. I can protect my computer against viruses by using an antivirus program.
6. Never trust an email from someone you don’t know.
7. A is for accepting

Words:

SICKNESS - ANTIVIRUS - PHISHING - VIRUS - COOKIE - ATTACHMENT - ACCEPTING - KARA - SMART - WINSTON - EMAIL - ADVICE - BLACKOWL - MESSAGE

Word Search:
Lesson 2:
Web Information

Overview:
The Internet has become a regular source for finding information, as there is an abundance of information available online. It is available with a single click of a button on a computer or even on a cell phone in your pocket. This availability has become a challenge for people searching for valid information as most information online cannot be trusted.

The main problem with the reliability of online information can be compared to the whispering game children play. The first person whispers something to the second person, who whispers it to the third and so on. This creates contamination where the message the last person receives is not the same as the original message. This is the same with information online. People give their own views and own accounts of whatever information you seek. This information isn’t always reliable or even true.

This lesson mainly focuses on information online that is not always legitimate. One method, amongst others, to verify the trustworthiness of online information is to consult two or more different websites or sources. Another is to verify the author. Children need to know that due care should be taken when finding information online as negligence in this area can lead to illegitimate information being shared.

Learning Objectives:
Primary: Understand why verifying the trustworthiness of online information is important.
Secondary:
1. Know why all information online is not trustworthy.
2. Be able to verify the validity of online information with different methods.

Materials: The adventures of Kara, Winston and the smart crew, Chapter 2 https://www.youtube.com/watch?v=GNf3OuUKWm

Procedure:
1. Introduce the concept of online information and recap lesson 1.
2. Watch video.
3. Reflect on video with class discussion.
4. Explain main lesson concepts.
5. Do class assessment to measure understanding and insight.

Discussion: Questions for class discussion:
1. What online sites are famous for finding information?
2. Why was Cookie afraid to go to the island?
3. What was the first sign that the information on the website was false?
4. What advice did the smart crew give?
5. Can anyone give other examples way of ensuring online information is true?
6. Should Cookie still be afraid?

Assessment: Fill in missing words and complete the word search assignment.
Lesson 2: Assessment

Instruction: Fill in the missing words in the following sentences. Upon completion, find the words in the word search. Make sure you find all of the words.

Questions:

1. ___________ and _________ are well known sites for finding information.
2. Information from an ________ author should not be trusted.
3. It is extremely important to check at least _______ websites when looking for information.
4. Don’t always ________ everything you read online.
5. It is ______ responsibility to ensure online information is true.
6. R is for ____________.

Words:

GOOGLE - WIKIPEDIA - ONE - TRUST - RELIABLE - FACEBOOK - KNOWN - DISTRUST - REAL - MOTHERS - UNKNOWN - YOUR - TWO

Word Search:
Lesson 2: Memorandum

Instruction: Fill in the missing words in the following sentences. Upon completion, find the words in the word search. Make sure you find all of the words.

Questions:

1. *Google* and *Wikipedia* are well known sites for finding information.
2. Information from only *unknown* author should not be trusted.
3. It is extremely important to check at least *two* websites when looking for information.
4. Don’t always *trust* everything you read online.
5. It is *your* responsibility to ensure online information is true.
6. R is for *reliable*.

Words:

| GOOGLE - WIKIPEDIA - ONE - TRUST - RELIABLE - FACEBOOK - KNOWN - DISTRUST - REAL - MOTHERS - UNKNOWN - YOUR - TWO |

Word Search:
Overview:
We live in the information age. We are connected with the cyber world through email, cell phones, online games, social networks, instant messaging applications and many more. All these different mediums were designed to make our lives a little easier. With all good things come the possible dangers and criminals trying to exploit these mediums.

Lesson 3 is all about sharing personal information online. Whether it be on social networks, in an email or whilst playing online games. The Internet has allowed a sense of anonymity and one can easily be conned into trusting someone portraying to be someone trustworthy.

It is essential that children know not to trust anyone when using the Internet and not give out details to fellow gamers or Facebook friends they accepted but don’t know, just like they would not give their details to someone on the street.

Learning Objectives:
Primary: Understand not to share information with strangers online.
Secondary:
1. Understand the concept of anonymity and how easy it is for a crook to disguise himself as someone trustworthy.
2. Know who you can trust on the Internet.

Materials:
Video: The adventures of Kara, Winston and the smart crew, Chapter 3 http://www.youtube.com/watch?v=HiygFwXnMzo

Procedure:
1. Overview of what information should be private. Recap lesson 2.
2. Watch video.
3. Reflect on video with class discussion.
4. Explain main lesson concepts.
5. Do class assessment to measure understanding and insight.

Discussion:
Questions for class discussion:
1. Why should you only play games with people you know?
2. Why do you think the gamer who invited Kara and Winston wanted this information?
3. What could have happened if this gamer found out their address and real names?
4. What advice did the smart crew give regarding talking to people online and sharing your information?
5. Where can crooks get your information other than online games?

Assessment:
Fill in missing words and complete the word search assignment.
Lesson 3: Assessment

Instruction: Fill in the missing words in the following sentences. Upon completion, find the words in the word search. Make sure you find all of the words.

Questions:

1. You can only trust your ________ on the Internet.
2. If you give out information online it may fall into the hands of ________.
3. Criminals will try to find out information such as your ________, ________ and telephone ________.
4. You should not talk to strangers when using platforms such as ________ games, and social media platforms like ________ and ________.
5. S is for ________.

Words:

FACEBOOK - ADDRESS - FRIENDS - ONLINE - STRANGERS - GAMERS - WHATSAPP - NUMBER - NAME - SAFE

Word Search:
Lesson 3: Memorandum

Instruction: Fill in the missing words in the following sentences. Upon completion, find the words in the word search. Make sure you find all of the words.

Questions:

1. You can only trust your friends on the Internet.
2. If you give out information online it may fall into the hands of strangers.
3. Criminals will try to find out information such as your address, name and telephone number.
4. You should not talk to strangers when using platforms such as online games, and social media platforms like facebook and whatsapp.
5. S is for safe.

Words:

FACEBOOK - ADDRESS - FRIENDS - ONLINE - STRANGERS - GAMERS - WHATSAPP - NUMBER - NAME - SAFE

Word Search:
# Lesson 4:
## Cyber Bullying

### Overview:
Cyber bullying is the deliberate act by an individual or a group, through the use of information technology communication mediums such as social media, emails, instant messaging etc., to cause harm to another. With the increase of access to technology, cyber bullying has become a common trait among teenagers. The Internet allows a smokescreen behind which aggressors of cyber bullying can hide whilst bullying their victims.

Some victims are negatively influenced by cyber bullying which can have a significant effect on them, such as an increase feeling of sadness, loss of interest in activities and a lower self-esteem. This lesson will focus on cyber bullying in order to explore why it is wrong, what should be done if you are a victim and what will happen should you be the aggressor of cyber bullying.

### Learning Objectives:
- **Primary:** Create an understanding of what cyber bullying is and why it is wrong.
- **Secondary:**
  1. Understand the consequences of cyber bullying.
  2. Know what should be done when you’re a victim of cyber bullying.

### Materials:
- Video: The adventures of Kara, Winston and the smart crew, Chapter 4
  [https://www.youtube.com/watch?v=ipD0IS4EUcl](https://www.youtube.com/watch?v=ipD0IS4EUcl)

### Procedure:
1. Introduce general concept of cyber bullying and recap lesson 3.
2. Watch video.
3. Reflect on video with class discussion.
4. Explain main lesson concepts.
5. Do class assessment to measure understanding and insight.

### Discussion:
Questions for class discussion:
1. What are some examples of cyber bullying?
2. Why is it wrong to bully someone online?
3. What advice are given by the smart crew about cyber bullying?
4. What should you do when you see someone are cyber bullied?
5. What will be the consequences if you are caught bullying someone online?

### Assessment:
Fill in missing words and complete the word search assignment.
Lesson 3: Assessment

Instruction: Fill in the missing words in the following sentences. Upon completion, find the words in the word search. Make sure you find all of the words.

Questions:

1. If you are caught bullying someone online, you will be ____________ and denied __________ to that site.
2. You should __________ tell someone when you are bullied.
3. __________ someone on Facebook is wrong.
4. __________ a photo of someone on Facebook is not an example of __________.
5. When you see someone being bullied you should __________ it to a __________ or __________.
6. T stands for __________.

Words:

GREETING - REPORTED - ALWAYS - TAUNTING - LIKING - REPORT - PARENT - NEVER - TEACHER - TELL - ACCESS - BULLYING - TERRIBLE

Word Search:
Lesson 4: Memorandum

Instruction: Fill in the missing words in the following sentences. Upon completion, find the words in the word search. Make sure you find all of the words.

Questions:

1. If you are caught bullying someone online, you will be reported and denied access to that site.
2. You should always tell someone when you are bullied.
3. Taunting someone on Facebook is wrong.
4. Liking a photo of someone on Facebook is not an example of bullying.
5. When you see someone being bullied you should report it to a parent or teacher.
6. T stands for tell.

Words:

GREETING - REPORTED - ALWAYS - TAUNTING -liking - REPORT - PARENT - NEVER - TEACHER - TELL - ACCESS - BULLYING - TERRIBLE

Word Search:
Lesson 5:  
Summary of SMART lessons

Overview:
The Internet with all of its advantages has brought with it many different issues which have impacted the safety of our online use. The video series of Kara, Winston and the SMART crew has touched on merely some of these cyber security issues. The issues looked at by this series included phishing, viruses, sharing of personal information, cyber bullying and finding valid information online.

In this lesson the last word of the SMART acronym is introduced, namely M for Meet. It completes the SMART guide for using the Internet. When using the Internet, children easily trust what they can see on the screen, possibly a profile. They are sometimes willing to meet these people in person which is extremely dangerous. As mentioned in lesson 3, a criminal can very easily disguise himself as someone whom he’s not. They create fake profiles then try and gain the trust of children in online platforms where after they try and lure the children to public meetings.

<table>
<thead>
<tr>
<th>Learning Objectives:</th>
<th>Primary:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Understand how to be SMART when using the Internet.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Secondary:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Understand the dangers of meeting strangers face-to-face.</td>
</tr>
<tr>
<td></td>
<td>2. Know what is meant by Safe, Meeting, Accepting, Reliable, Tell</td>
</tr>
</tbody>
</table>

| Materials: | Video: The adventures of Kara, Winston and the smart crew, Chapter 5 [https://www.youtube.com/watch?v=HI0US7LgGeQ](https://www.youtube.com/watch?v=HI0US7LgGeQ) |

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Watch video.</td>
</tr>
<tr>
<td></td>
<td>3. Reflect on video with class discussion.</td>
</tr>
<tr>
<td></td>
<td>4. Explain main lesson concepts.</td>
</tr>
<tr>
<td></td>
<td>5. Do class assessment to measure understanding and insight.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Discussion:</th>
<th>Questions for class discussion:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Why is it wrong to meet up with someone you met online?</td>
</tr>
<tr>
<td></td>
<td>2. What dangers does meeting up with a stranger hold?</td>
</tr>
<tr>
<td></td>
<td>3. How should we use the Internet? (SMART)</td>
</tr>
<tr>
<td></td>
<td>4. What do each of the SMART words mean?</td>
</tr>
<tr>
<td></td>
<td>5. Why is it important to use the Internet in a smart manner?</td>
</tr>
</tbody>
</table>

| Assessment: | Fill in the missing word and word search assignment |

Questions:

1. The adventures of Kara, Winston and the smart crew has taught us to use the Internet in a ________ way.
2. SMART is an acronym for ________, ________, ________, ________, ________, and ________.
3. A fake ________ can make someone online seem as if they are someone trustworthy.
4. When someone you don’t know tries to organise a meeting with you, you should tell your ________.
5. You should always take an adult with you when you meet a friend in ________ for the first time.

Words:

SMART - SAFE - DOG - PROFILE - TELL - RELIABLE - PARENT - PUBLIC - MEET - ACCEPTING - RISKY - NAME

Word Search:
Lesson 5: Memorandum

Instruction: Fill in the missing words in the following sentences. Upon completion, find the words in the word search. Make sure you find all of the words.

Questions:

1. The adventures of Kara, Winston and the smart crew has taught us to use the Internet in a **smart** way.
2. SMART is an acronym for **safe**, **meet**, **accepting**, **reliable** and **tell**.
3. A fake **profile** can make someone online seem as if they are someone trustworthy.
4. When someone you don’t know tries to organise a meeting with you, should tell your **parent**.
5. You should always take an adult with you when you meet a friend in **public** for the first time

Words:

SMART - SAFE - DOG - PROFILE - TELL - RELIABLE - PARENT - PUBLIC - MEET - ACCEPTING - RISKY - NAME

Word Search:
Overview:
Information contained in a user’s account is confidential and if attackers get access to this information it can have serious consequences. The first line of defence in your account is the use of a password. Hackers have become more sophisticated at password “cracking” and for this reason it is important to ensure a strong password is used.

When strong passwords are not used, hackers can get access to a variety of personal information such as ID number, contact details, address details and banking details. Also, when they are able access a social media account, they can post false information on the victims profile or send messages to their friends list in an attempt to destroy the reputation of the victim or gain information from friends of the victim.

This lesson will take a look at the importance for strong passwords.

<table>
<thead>
<tr>
<th>Learning Objectives:</th>
<th>Primary:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know and understand the importance of strong passwords.</td>
<td></td>
</tr>
<tr>
<td>Secondary:</td>
<td>1. Understand what a strong password is. 2. Understand the consequences of using a weak password.</td>
</tr>
</tbody>
</table>

| Materials: | Video: UYN The Password Rap 2000k [https://www.youtube.com/watch?v=T0Q5b-pzhD8](https://www.youtube.com/watch?v=T0Q5b-pzhD8) |

| Procedure: | 1. Overview of password creation. 2. Watch video. 3. Reflect on video with class discussion. 4. Explain main lesson concepts. 5. Do class assessment to measure understanding and insight. |

| Discussion: | Questions for class discussion: 1. What information can a hacker get access to when your password has been cracked? 2. What should your password not be? 3. What should your password contain to make it more difficult to crack? 4. How often should you change your password? 5. Who can you trust your password with? |

| Assessment: | Worksheet: Comprehension Test |
Lesson 6: Assessment

*Instruction: Answer the questions to the following scenarios.*

**Freddy just got into a new school. He did not know anyone and felt alone. One day a boy came to Freddy and asked him kindly if he wanted to play with him. Freddy smiled and said yes. They then went off and played. Freddy was shy at the start, but as they played along he started to get comfortable. Freddy’s new friend, Jeremy, then dared him to climb a big tree with him. Jeremy went first and climbed the tree to the top. Freddy followed him and made it to the top as well. Feeling brave making it to the top, Freddy asked Jeremy if he has Facebook. Jeremy said yes and asked him to invite him on Facebook so that they can chat and play Facebook games. Freddy said he does not know how to play Facebook games. Jeremy suggested him to give him his password and he will set up the game for him on Facebook. Freddy was so excited about the game and kindly gave it to Jeremy.**

1. Why should Freddy not have told his new friend his Facebook password?
   ____________________________________________________________________________
   ____________________________________________________________________________

2. If you were Freddy what would you have done?
   ____________________________________________________________________________
   ____________________________________________________________________________

3. Who can Freddy trust his password with?
   ____________________________________________________________________________
   ____________________________________________________________________________

4. What can happen to Freddy because he gave his password to Jeremy?
   ____________________________________________________________________________
   ____________________________________________________________________________
   ____________________________________________________________________________

**Shaun just got a new game, Online Shooter 5, and he was so excited to play with his friends online. He installed the game and when the installation was completed, the game asked him to create a password. Because Shaun was so excited, he was lazy to create a good password and made the password “1234”. He quickly went online and played with his friends and collected awesome guns. The next day Shaun went online again to play the game and realized all the guns he collected the previous day were gone. He was very sad as he worked hard to collect them. He does not know what went wrong.**

1. What do you think happened?
   ____________________________________________________________________________
   ____________________________________________________________________________

2. Give Shaun suggestions how to create a strong password?
   ____________________________________________________________________________
   ____________________________________________________________________________

3. Give an example of a strong password?
   ____________________________________________________________________________
   ____________________________________________________________________________

4. What are also bad passwords to use?
   ____________________________________________________________________________
Lesson 6: Assessment

Instruction: Answer the questions to the following scenarios.

Freddy just got into a new school. He did not know anyone and felt alone. One day a boy came to Freddy and asked him kindly if he wanted to play with him. Freddy smiled and said yes. They then went off and played. Freddy was shy at the start, but as they played along he started to get comfortable. Freddy’s new friend, Jeremy, then dared him to climb a big tree with him. Jeremy went first and climbed the tree to the top. Freddy followed him and made it to the top as well. Feeling brave making it to the top, Freddy asked Jeremy if he has Facebook. Jeremy said yes and asked him to invite him on Facebook so that they can chat and play Facebook games. Freddy said he does not know how to play Facebook games. Jeremy suggested him to give him his password and he will set up the game for him on Facebook. Freddy was so excited about the game and kindly gave it to Jeremy.

1. Why should Freddy not have told his new friend his Facebook password?
   *Any applicable answer is acceptable. For example Jeremy can now access Freddy’s details or post something on his behalf.

2. If you were Freddy what would you have done?
   *State that Freddy should not give his password out.

3. Who can Freddy trust his password with?
   Only his parents/guardians.

4. What can happen to Freddy, because he gave his password to Jeremy?
   Jeremy can post inappropriate status messages or send inappropriate messages to Freddy’s friends / Jeremy can also give out Freddy’s password to others / He can get Freddy’s personal details.

Shaun just got a new game, Online Shooter 5, and he was so excited to play with his friends online. He installed the game and when the installation was completed, the game asked him to create a password. Because Shaun was so excited, he was lazy to create a good password and made the password “1234”. He quickly went online and played with his friends and collected awesome guns. The next day Shaun went online again to play the game and realised all the guns he collected the previous day were gone. He was very sad as he worked hard to collect them. He does not know what went wrong.

1. What do you think happened?
   His password was cracked by someone who then took all of his items from his character

2. Give Shaun suggestions how to create a strong password?
   Construct an easy to remember sentence and use the first letter of each word as the password / Must be at least 8 characters long / Mix numbers, letters and symbols.

3. Give an example of a strong password?
   *Any password that matches the recommendations mentioned in this lesson.

4. What are also bad passwords to use?
   Anything that is easy to figure out or that refers to you such as your name surname date of birth or even pets name.
**Overview:**
Viruses are malicious software programs that, when executed, perform harmful activities on the infected hosts. The first ever computer virus was the “Creeper virus” which was detected in the early 1970’s. Not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without the user's consent.

In today’s technological world file sharing is prominent. Sharing music or movies with a friend, sending photos using email and downloading programs from public websites are some of the file sharing activities taking place.

This lesson places focus on protection from viruses by keeping an up to date antivirus program on your computer. It is very important that the antivirus program is kept updated as new viruses surface every day. Having an up to date antivirus isn’t a 100% secure solution. Users need to be wary and alert when copying or downloading files.

**Learning Objectives:**

| Primary: | Comprehend the importance of an antivirus program to combat the spread of viruses. |
| Secondary: | 1. Understand the dangers of file downloading and copying.  
2. Know why antivirus software is needed and why it is important to keep it updated. |

**Materials:**
- Video: UYN Don't Open That File 2000k
  https://www.youtube.com/watch?v=nlx4wRkssRo

**Procedure:**

2. Watch video.  
3. Reflect on video with class discussion.  
4. Explain main lesson concepts.  
5. Do class assessment to measure understanding and insight.

**Discussion:**

Questions for class discussion:  
1. What does a virus do?  
2. How can your computer be infected with a virus?  
3. Is an email you receive from a friend always safe and virus free?  
4. How can you stop a virus from infecting your computer?  
5. Why should an antivirus program be updated?  
6. Will an antivirus program always detect the viruses?

**Assessment:**
- Worksheet: Comprehension Test
Lesson 7: Assessment

*Instruction: Answer the questions to the following scenarios.*

Willy Wonka sat in front of his computer one day typing out a new recipe for a brand new top secret treat. He struggled to find out what ingredients he needed to add to one of the layers of his new chocolaty treat. He emailed his long-time friend, the Baker Man, asking for some advice. After a little while the Baker Man emailed him a list of suggestions. Upon opening the file, Willy’s screen went black and a big X appeared soon after. He was very frightened that he might have lost all of his recipes, so he called up the computer guy who said that a virus caused his computer to crash. It was a very sad day at the chocolate factory.

1. What do you think went wrong with Mr. Wonka’s computer?

2. What was wrong with the file Mr. Wonka received via email from the Baker Man?

3. Was it the Baker Man’s fault that Mr. Wonka’s computer crashed?

4. What could Mr. Wonka have done to prevent a virus crashing his computer?

5. What were the consequences of Mr. Wonka not having up to date antivirus software?

It is Timmy’s birthday today and his parents decided to get him the latest gaming computer for his special day. Timmy could not wait to install all of the latest games and start playing. The next day during lunch time at school, Timmy and his friend, Mark, discussed all of the games he can play, but Timmy said that he could not afford all the games at once. Mark suggested to Timmy that he should come to his house after school and copy all of his games to a flash-drive and install them on his computer. Timmy got home late that afternoon, scanned the flash-drive with his antivirus program and after getting the all clear installed the games on his computer. The next day when Timmy wanted to play, his computer wasn’t working anymore. He knew his parent would be very cross with him, but he didn’t know what went wrong.

1. What do you think caused Timmy’s computer to break?

2. Where did Timmy get the possible virus from?

3. Did Timmy have an antivirus program?

4. Why do you think the antivirus was ineffective?
Lesson 7: Memorandum

Instruction: Answer the questions to the following scenarios.

Willy Wonka sat in front of his computer one day typing out a new recipe for a brand new top secret treat. He struggled to find out what ingredients he needed to add to one of the layers of his new chocolaty treat. He emailed his long-time friend, the Baker Man, asking for some advice. After a little while the Baker Man emailed him a list of suggestions. Upon opening the file, Willy’s screen went black and a big X appeared soon after. He was very frightened that he might have lost all of his recipes, so he called up the computer guy who said that a virus caused his computer to crash. It was a very sad day at the chocolate factory.

1. What do you think went wrong with Mr. Wonka’s computer?
   
   It was infected by a virus.

2. What was wrong with the file Mr. Wonka received via email from the Baker Man?
   
   It contained a virus.

3. Was it the Baker Man’s fault that Mr. Wonka’s computer crashed?
   
   No, Mr. Wonka should have had the necessary antivirus program to prevent something like this.

4. What could Mr. Wonka have done to prevent a virus crashing his computer?
   
   Have an up to date antivirus program that can scan the email for viruses.

5. What were the consequences of Mr. Wonka not having up to date antivirus software?
   
   A very dangerous virus infected his computer and it crashed.

It is Timmy’s birthday today and his parents decided to get him the latest gaming computer for his special day. Timmy could not wait to install all of the latest games and start playing. The next day during lunch time at school, Timmy and his friend, Mark, discussed all of the games he can play, but Timmy said that he could not afford all the games at once. Mark suggested to Timmy that he should come to his house after school and copy all of his games to a flash-drive and install them on his computer. Timmy got home late that afternoon, scanned the flash-drive with his antivirus program and after getting the all clear installed the games on his computer. The next day when Timmy wanted to play, his computer wasn’t working anymore. He knew his parent would be very cross with him, but he didn’t know what went wrong.

1. What do you think caused Timmy’s computer to break?
   
   His antivirus program was not up to date when he scanned the flashed drive.

2. Where did Timmy get the possible virus from?
   
   From the flash drive.

3. Did Timmy have an antivirus program?
   
   Yes.

4. Why do you think the antivirus was ineffective?
   
   His antivirus program was not up to date.
Lesson 8: 
Accepting friend requests

Overview: 
At this young age, children are very vulnerable as they trust others easily. They are also very naïve. Most children are on Facebook or other social media platforms. A person can be found on these platforms by simply searching their names. Your own information stays private until you confirm that person’s friend request. By confirming the friend request, you confirm that you know that person and that you trust that person to see your personal information and daily activities.

This lesson, the first of a new cartoon series, addresses the issue of friend requests and emphasises children’s sometimes naïve attitude towards accepting friend requests on social media. The main message of the video explains that by confirming a Facebook friend, you invite them into your life. It is important that children know what consequences accepting a stranger on social media may have.

Learning Objectives: 
Primary: 
Comprehend the dangers of accepting strangers on social media.

Secondary: 
1. Know why it is important to only accept people you know.
2. Understand that you invite people into your life when you accept them on social media.

Materials: 
Video: Funmoods’ Online Safety Kit - Little Red Riding Mood: Chapter 1. 
https://www.youtube.com/watch?v=KGr_KFiCX4s

Procedure: 
1. Overview of social media and friend requests.
2. Watch video.
3. Reflect on video with class discussion.
4. Explain main lesson concepts.
5. Do class assessment to measure understanding and insight.

Discussion: 
Questions for class discussion:
1. What social media platforms are available?
2. Who should you not accept as a friend?
3. What may the consequences be of accepting a stranger?
4. What happened after Little Red accepted the friend request?
5. What did you notice about the profile photo the wolf had on his profile?
6. How easy is it for someone to make a fake Facebook profile?

Assessment: 
Worksheet: Comprehension Test
Lesson 8: Assessment

Instruction: Answer the question to the following scenarios.

Chelsea has 545 friends on Facebook. She recently received an invitation from a boy named Carl. Upon opening the invitation, she noticed that they had 65 mutual friends. She didn’t know anyone named Carl, but they do have 65 mutual friends so she wasn’t too worried about accepting his request. A few weeks later it was Chelsea’s birthday and she had a big party planned. A week before the party she created an event and invited some of her close friends. Unknowingly, the event she created was publically visible to all her Facebook friends, which normally wouldn’t be a problem. When the big day finally arrived, Chelsea was ready to celebrate. She had already received a lot of birthday wishes on her Facebook wall. That afternoon the music was playing, the food and games were ready and Chelsea was waiting for her friends to show up for her party. After all of her friends already showed, Chelsea’s mom called and asked why there were other people at the door saying they were invited to the party. One of these people, included a boy named Carl. Chelsea was left embarrassed and in big trouble, this on her big day.

1. Why do you think Chelsea and Carl had so many mutual friends?
   ________________________________________________________________

2. Did Chelsea make the right decision in accepting Carl’s friend request?
   ________________________________________________________________

3. Why is it wrong to accept strangers on Facebook?
   ________________________________________________________________

4. What were the consequences of Chelsea’s bad decision?
   ________________________________________________________________

5. Do you think Chelsea knows the 545 people she is friends with?
   ________________________________________________________________

6. What would you suggest Chelsea do to protect her social media information?
   ________________________________________________________________
Lesson 8: Memorandum

Instruction: Answer the question to the following scenarios.

Comprehension test:

Chelsea has 545 friends on Facebook. She recently received an invitation from a boy named Carl. Upon opening the invitation, she noticed that they had 65 mutual friends. She didn’t know anyone named Carl, but they do have 65 mutual friends so she wasn’t too worried about accepting his request. A few weeks later it was Chelsea’s birthday and she had a big party planned. A week before the party she created an event and invited some of her close friends. Unknowingly, the event she created was publicly visible to all her Facebook friends, which normally wouldn’t be a problem. When the big day finally arrived, Chelsea was ready to celebrate. She had already received a lot of birthday wishes on her Facebook wall. That afternoon the music was playing, the food and games were ready and Chelsea was waiting for her friends to show up for her party. After all of her friends already showed, Chelsea’s mom called and asked why there were other people at the door saying they were invited to the party. One of these people, included a boy named Carl. Chelsea was left embarrassed and in big trouble, this on her big day.

1. Why do you think Chelsea and Carl had so many mutual friends?
   *Chelsea has a lot of friends on Facebook many of whom she probably doesn’t know personally*

2. Did Chelsea make the right decision in accepting Carl’s friend request?
   *No, she should have ignored the friend request, because she does not know Carl*

3. Why is it wrong to accept strangers on Facebook?
   *They are able to see your profile details and activities you post*

4. What were the consequences of Chelsea’s bad decision?
   *Carl posted her birthday party to the public and everyone was able to see it so uninvited people came to her party*

5. Do you think Chelsea knows the 545 people she is friends with?
   *No, not everyone*

6. What would you suggest Chelsea do to protect her social media information?
   *She must delete friends on her Facebook that she doesn’t know. / Put her profile on private. / Ignore friend request from people she doesn’t know.*
**Overview:**
Privacy is very much overlooked in today's social media frenzy. Most people using social media do not know who can share the content they share on a daily basis. Most social media website owners know that privacy is very important, but they do not generate much awareness amongst their users about adjusting their privacy settings. The users are thus left vulnerable and without them knowing, can have strangers see their personal posts and information.

This lesson is all about privacy settings. It emphasises the importance of adjusting your privacy settings to your desired level. You need to choose what you show the world. Children need to be educated on how they can change their privacy settings.

<table>
<thead>
<tr>
<th>Learning Objectives:</th>
<th>Primary: Understand privacy settings on social media platforms.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secondary: 1. Know why it is important to change privacy settings. 2. Learn how to choose privacy settings on Facebook.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Materials:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video: Funmoods- Online Safety- Little Red Riding Mood: Chapter 2. <a href="https://www.youtube.com/watch?v=Dn1Jmqecvk">https://www.youtube.com/watch?v=Dn1Jmqecvk</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Procedure:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Overview of privacy. Recap Lesson 8. 2. Watch video. 3. Reflect on video with class discussion. 4. Explain main lesson concepts. 5. Do class assessment to measure understanding and insight.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Discussion:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Questions for class discussion: 1. What is privacy? 2. Name some examples of private information? 3. How can you prevent people from seeing your private information? 4. Why should you adjust your privacy settings on Facebook? 5. Will adjusting privacy settings protect your information from Facebook friends you accepted but don't know? 6. How should you deal with people you don't know on social media?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assessment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worksheet: Match setting with content</td>
</tr>
</tbody>
</table>
Lesson 9: Assessment

Instruction: Match the correct privacy setting with the content. Write the letter of the correct answer next to the appropriate content.

<table>
<thead>
<tr>
<th>Facebook Content:</th>
<th>Correct Privacy Setting:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Address and telephone number</td>
<td>A  Everyone</td>
</tr>
<tr>
<td>2  Checked in at current location</td>
<td>B  Friends of friends</td>
</tr>
<tr>
<td>3  New profile photo</td>
<td>C  Friends only</td>
</tr>
<tr>
<td>4  Album of family holiday</td>
<td>D  Family only</td>
</tr>
<tr>
<td>5  Email address</td>
<td></td>
</tr>
<tr>
<td>6  Relationship status</td>
<td></td>
</tr>
<tr>
<td>7  Birthday</td>
<td></td>
</tr>
<tr>
<td>8  Family members</td>
<td></td>
</tr>
<tr>
<td>9  Status message</td>
<td></td>
</tr>
</tbody>
</table>

Instruction: Place the steps for changing your privacy settings in the correct order by writing the appropriate letter next to the step.

Step 1: _____

Step 2: _____

Step 3: _____

Step 4: _____

Step 5: _____
Lesson 9: Memorandum

*Instruction:* Match the correct privacy setting with the content. Write the letter of the correct answer next to the appropriate content.

<table>
<thead>
<tr>
<th>Facebook Content:</th>
<th>Correct Privacy Setting:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Address and telephone number</td>
<td>D</td>
</tr>
<tr>
<td>2 Checked in at current location</td>
<td>C</td>
</tr>
<tr>
<td>3 New profile photo</td>
<td>B</td>
</tr>
<tr>
<td>4 Album of family holiday</td>
<td>C</td>
</tr>
<tr>
<td>5 Email address</td>
<td>C</td>
</tr>
<tr>
<td>6 Relationship status</td>
<td>B</td>
</tr>
<tr>
<td>7 Birthday</td>
<td>C</td>
</tr>
<tr>
<td>8 Family members</td>
<td>C</td>
</tr>
<tr>
<td>9 Status message</td>
<td>C</td>
</tr>
</tbody>
</table>

*Instruction:* Place the steps for changing your privacy settings in the correct order by writing the appropriate letter next to the step.

Step 1: ____C____

Step 2: ____B____

Step 3: ____D____

Step 4: ____A____

Step 5: ____E____
**Overview:**

Cyber bullying is the deliberate act by an individual or a group, through the use of information technology communication mediums such as social media, emails, instant messaging etc., to cause harm to another. With the increase of access to technology, cyber bullying has become a common trait among teenagers. The Internet allows a smokescreen behind which aggressors of cyber bullying can hide whilst bullying their victims.

Some victims are negatively influenced by cyber bullying which can have a significant effect on them, such as an increase feeling of sadness, loss of interest in activities and a lower self-esteem. This lesson will focus on cyber bullying in order to explore why it is wrong, what should be done if you are a victim and what will happen should you be the aggressor of cyber bullying.

This lesson is all about cyber bullying. It emphasises the importance of reporting cyber bullying to a parent or teacher.

<table>
<thead>
<tr>
<th>Learning Objectives:</th>
<th>Primary:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an understanding of what cyber bullying is and why it is wrong.</td>
<td></td>
</tr>
<tr>
<td>Secondary:</td>
<td></td>
</tr>
<tr>
<td>1. Create an understanding of what cyber bullying is and why it is wrong.</td>
<td></td>
</tr>
<tr>
<td>2. Know what should be done when you’re a victim of cyber bullying.</td>
<td></td>
</tr>
</tbody>
</table>

| Materials: | Video: Funmoods - Online Safety- Little Red Riding Mood- Chapter 3 [https://www.youtube.com/watch?v=elYv-pZVgYo](https://www.youtube.com/watch?v=elYv-pZVgYo) |

| Procedure: |
| 2. Watch video |
| 3. Reflect on video with class discussion |
| 4. Explain main lesson concepts |
| 5. Do class assessment to measure understanding and insight |

| Discussion: | Questions for class discussion: |
| 1. What are some examples of cyber bullying? |
| 2. Why is it wrong to bully someone online? |
| 3. Why shouldn’t you keep quiet about being bullied? |
| 4. What should you do when you see someone being cyber bullied? |
| 5. To whom should you report cyber bullying? |

| Assessment: | Worksheet: True/False for bullying activities and essay. |
Lesson 10: Assessment

True/False Questions:

*Instruction: State whether the action is a form of cyber bullying by writing true or false.*

<table>
<thead>
<tr>
<th>ACTION</th>
<th>TRUE/FALSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Facebook friend making a joke about your bad hair day on Facebook.</td>
<td></td>
</tr>
<tr>
<td>A Facebook friend spreading rumours about you on his wall every day.</td>
<td></td>
</tr>
<tr>
<td>A friend asking for you Twitter password.</td>
<td></td>
</tr>
<tr>
<td>A Facebook friend uploading an edited picture of you after a birthday party.</td>
<td></td>
</tr>
<tr>
<td>A Twitter follower constantly making bad comments about your tweets and embarrassing you.</td>
<td></td>
</tr>
<tr>
<td>A stranger on Facebook repeatedly sends you nasty messages.</td>
<td></td>
</tr>
<tr>
<td>A Facebook friend tags you in pictures of funny animals, saying you look like them.</td>
<td></td>
</tr>
</tbody>
</table>

Essay:

*Instruction: Shortly tell someone why cyber bullying is wrong and what they should do if they are a victim.*

__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
Lesson 10: Memorandum

True/False Questions:

*Instruction: State whether the action is a form of cyber bullying by writing true or false.*

<table>
<thead>
<tr>
<th>ACTION</th>
<th>TRUE/FALSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Facebook friend making a joke about your bad hair day on Facebook.</td>
<td>True</td>
</tr>
<tr>
<td>A Facebook friend spreading rumours about you on his wall every day.</td>
<td>True</td>
</tr>
<tr>
<td>A friend asking for you Twitter password.</td>
<td>False</td>
</tr>
<tr>
<td>A Facebook friend uploading an edited picture of you after a birthday party.</td>
<td>False</td>
</tr>
<tr>
<td>A Twitter follower constantly making bad comments about your tweets and embarrassing you.</td>
<td>True</td>
</tr>
<tr>
<td>A stranger on Facebook repeatedly sends you nasty messages.</td>
<td>True</td>
</tr>
<tr>
<td>A Facebook friend tags you in pictures of funny animals, saying you look like them.</td>
<td>True</td>
</tr>
</tbody>
</table>

Essay:

*Instruction: Shortly tell someone why cyber bullying is wrong and what they should do if they are a victim.*

- Cyber bullying can influence someone else emotions. Make them sad.
- Words can hurt someone.
- Cyber bullying can leave someone not wanting to take part in social activities or even go to school.
- Some have committed suicide of being a victim of cyber bullying.
- They can get into trouble when they cyber bully.
- You should not take bad comments or any form of cyber bullying literally.
- Save evidence if you get cyber bullied.
- Don’t reply to the person who cyber bullies you. Ignore them.
- Delete and block the person who cyber bullies you.
- Speak to your parents/guardians or teacher when you get cyber bullied.
Overview:
Instant Messaging is a phenomenon that changed the way we communicate. IM for short, it uses the Internet to send and receive text messages. It has become a major threat to the normal SMS’s in that you don’t pay per message, but merely for the Internet data you use. Popular platforms include MXIT, WhatsApp, BBM and WeChat. Latest IM’s applications allow one to even send pictures and video.

With this advantageous technology also come new threats. Most of these applications allow you to enter “chat rooms” where you can meet new people and make new friends. Children are particularly vulnerable in that criminals pose as someone friendly online to gain their trust and then try to meet them in person offline, which is extremely dangerous.

This lesson focusses on IM, but in particularly the dangers of meeting people you don’t know. Children need to know that they shouldn’t share information online, not to trust strangers they meet on IM applications and to never meet up with strangers. This lesson emphasises that you shouldn’t trust anyone online and most importantly should not meet with them in person. If someone wants to meet you in person you should immediately inform a parent or teacher.

Learning Objectives:
Primary:
Understand the danger of meeting online friends in person.

Secondary:
1. Know what to do if someone requests to meet you in person.
2. Understand consequences of meeting a stranger in person.

Materials:
Video: Faux Paw’s Adventures in the Internet
https://www.youtube.com/watch?v=gPse7dcXwrU

Procedure:
1. Overview of danger of online friendships.
2. Watch video
3. Reflect on video with class discussion
4. Explain main lesson concepts
5. Do class assessment to measure understanding and insight

Discussion:
Questions for class discussion:
1. What are some examples of cyber bullying?
2. Why is it wrong to bully someone online?
3. Why shouldn’t you keep quiet about being bullied?
4. What should you do when you see someone being cyber bullied?
5. To whom should you report cyber bullying?

Assessment:
Worksheet: Match column A with answer in B and comprehension test
Lesson 11: Assessment

Match Columns:

Instruction: Match the correct reaction in the second column with the scenario in the first by drawing a line.

<table>
<thead>
<tr>
<th>SCENARIO:</th>
<th>BEST WAY TO REACT:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Online friend ask to meet in person</td>
<td>Unfriend that person</td>
</tr>
<tr>
<td>B Online friend wants to know your address</td>
<td>Give it to him but be weary</td>
</tr>
<tr>
<td>C Online friend asks for your Gamer nickname</td>
<td>Report him to the website</td>
</tr>
<tr>
<td>D Online friend asks for your email address</td>
<td>Only if he’s a trusted friend</td>
</tr>
<tr>
<td>E Online friend sends you spam messages</td>
<td>Tell your parent or teacher</td>
</tr>
<tr>
<td>F Online friend wants to visit you</td>
<td>Say no, and tell a parent.</td>
</tr>
<tr>
<td>G Online friend asks you for photos</td>
<td>Take his so you can invite him for a game</td>
</tr>
</tbody>
</table>

Instruction: Answer the questions to the following scenario.

One night whilst Kenny was lying in bed chatting to his friends on MXIT, one of them suggested they join this new chat room he discovered earlier in the day. Kenny’s friend told him that he met a lot of new people and made new friends. Kenny was very excited and while texting in the chat room, one of the guys named Boogy11 suggested they start a private chat session. Kenny was glad that he made a new friend. After chatting to Boogy11 for a while Kenny noticed that Boogy11 was asking a lot of questions. Boogy11 wanted to know Kenny’s real name and later asked to meet Kenny in person.

1. Why do you think Boogy11 asked to talk to Kenny privately?

__________________________________________________________________________________
__________________________________________________________________________________

2. Why shouldn’t Kenny give any of his information to Boogy11?

__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________

3. Was Kenny’s friend’s suggestion to join a chatroom safe? Why?

__________________________________________________________________________________
__________________________________________________________________________________

4. Why is it easy for criminals to disguise themselves in chatrooms?

__________________________________________________________________________________
__________________________________________________________________________________

5. What could have happened if Kenny decided to meet with Boogy11 in person?

__________________________________________________________________________________
__________________________________________________________________________________
Lesson 11: Memorandum

Match Columns:

Instruction: Match the correct reaction in the second column with the scenario in the first by drawing a line.

<table>
<thead>
<tr>
<th>SCENARIO:</th>
<th>BEST WAY TO REACT:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Online friend ask to meet in person</td>
<td>Unfriend that person</td>
</tr>
<tr>
<td>B Online friend wants to know your address</td>
<td>Give it to him but be weary</td>
</tr>
<tr>
<td>C Online friend asks for your Gamer nickname</td>
<td>Report him to the website</td>
</tr>
<tr>
<td>D Online friend asks for your email address</td>
<td>Only if he’s a trusted friend</td>
</tr>
<tr>
<td>E Online friend sends you spam messages</td>
<td>Tell your parent or teacher</td>
</tr>
<tr>
<td>F Online friend wants to visit you</td>
<td>Say no, and tell a parent.</td>
</tr>
<tr>
<td>G Online friend asks you for photos</td>
<td>Take his so you can invite him for a game</td>
</tr>
</tbody>
</table>

Comprehension Test:

Instruction: Answer the questions to the following scenario.

One night whilst Kenny was lying in bed chatting to his friends on MXIT, one of them suggested they join this new chat room he discovered earlier in the day. Kenny’s friend told him that he met a lot of new people and made new friends. Kenny was very excited and while texting in the chat room, one of the guys named Boogy11 suggested they start a private chat session. Kenny was glad that he made a new friend. After chatting to Boogy11 for a while Kenny noticed that Boogy11 was asking a lot of questions. Boogy11 wanted to know Kenny’s real name and later asked to meet Kenny in person.

1. Why do you think Boogy11 asked to talk to Kenny privately?
   *He wanted to lure Kenny away from the chat room where others can read all the messages.*

2. Why shouldn’t Kenny give any of his information to Boogy11?
   *It is private information and in the wrong hands it can lead to dire consequences*

3. Was Kenny’s friend’s suggestion to join a chat room safe? Why?
   *No, there are a lot of criminals using these chat rooms posing as friends that want to get people’s personal information*

4. Why is it easy for criminals to disguise themselves in chat rooms?
   *They make a fake name with a fake picture*

5. What could have happened if Kenny decided to meet with Boogy11 in person?
   *He could have been a criminal and kidnapped Kenny*
Overview:
Video games are becoming more detailed and complex. With the increase in graphics detail, more realistic characters and greater challenges, it causes more children and teens to rather want to play the latest games than to go out with friends or participating in some sport activities. This can lead to game addiction. This can lead to negative symptoms such as poor health, poor eating habits and bad social reputation.

This lesson will create awareness about online game addiction and what the negative effects of game addiction are. Furthermore, it will discuss what steps can be taken to avoid becoming addicted to games.

Learning Objectives:
Primary: The purpose of this lesson is to learn about online game addiction and how to avoid it.
Secondary: 1. Understand what game addiction is and the causes of it. 2. Know how to avoid game addiction.

Materials: Video: Faux Paw Goes to the Games https://www.youtube.com/watch?v=hGfjyDALM2Q

Procedure:
1. Overview of online gaming. Recap lesson 11.
2. Watch video.
3. Reflect on video with class discussion.
4. Explain main lesson concepts.
5. Do class assessment to measure understanding and insight.

Discussion:
Questions for class discussion:
1. What is meant by online gaming?
2. How do you get addicted into online gaming?
3. How do you avoid getting addicted to online gaming?
4. When do you know you are addicted to online gaming?
5. What are the effects of being addicted to online gaming?
6. How do you get out of online game addiction?

Assessment:
Worksheet: Cross-word puzzle
Lesson 12: Assessment

Instruction: Complete the following crossword puzzle by filling in the missing words from the sentences and matching the word in the crossword puzzle.

1. Playing too many games can be bad for your ________, like causing headaches and bad hygiene.
2. Online gaming addiction can cause bad ________ status.
3. The best tool to cure online game addiction is to ________ to someone in person such as a family member about it.
4. Playing games on your ________ can also cause online game addiction.
5. Online gaming can become ________.
6. You should not play games for ________ periods of time.

1.  
2.  
3.  
4.  
5.  
6.  

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lesson 12: Memorandum

Instruction: Complete the following crossword puzzle by filling in the missing words from the sentences and matching the word in the crossword puzzle.

1. Playing too many games can be bad for your **health** like causing headaches and bad hygiene.
2. Online gaming addiction can cause bad **social** status.
3. The best tool to cure online game addiction is to **speak** to someone in person such as a family member about it.
4. Playing games on your **phone** can also cause online game addiction.
5. Online gaming can become **addictive**.
6. You should not play for **long** periods of time games.

```
  D I C T I V E
  I A K
  H L O N G
  O P
```

```
  P H O N E
  A D D I C T I V E
```

```
  L I A
  T A K
  H
```
# Lesson 13: Illegal Downloads

## Overview:
Illegal downloading is the practice of retrieving digital media such as computer programs, multimedia (music, movies etc.) and e-books for which you don't have rights to - for free online. One can face dire consequences when downloading illegal media and face time in jail. Further, by downloading these media files, one exposes your computer to malicious attacks such as viruses, spyware and other harmful software. Because these media files are easily available, one does not necessarily realise the consequences of downloading it. It is important to raise awareness to children about the consequences they can face when participating in illegal downloads.

For this lesson, illegal downloading will be defined and explained with examples. Further, the consequences of it will be discussed to give the children an understanding of the consequences of downloading illegal media.

## Learning Objectives:
**Primary:**
- Understanding what illegal downloads are and the consequences of it.

**Secondary:**
1. Knowing that downloading media to which you don’t have rights for is a criminal offense.
2. Knowing when a download is illegal.

## Materials:
- Video: Faux Paw's Dangerous Download [https://www.youtube.com/watch?v=N1xFUw3bW10](https://www.youtube.com/watch?v=N1xFUw3bW10)

## Procedure:
2. Watch video
3. Reflect on video with class discussion
4. Explain main lesson concepts
5. Do class assessment to measure understanding and insight

## Discussion:
**Questions for class discussion:**
1. What is illegal downloads?
2. Give examples of illegal downloads?
3. What is the consequences of illegally downloading media?
4. How do you know if a download is legal or not?
5. What is peer-to-peer downloading

## Assessment:
**Worksheet: Cross-word puzzle**
Lesson 13: Assessment

Instruction: Complete the following crossword puzzle by filling in the missing words from the sentences and matching the word in the crossword puzzle.

1. Peer-to-peer downloading is _________.
2. ________ is an example of media.
3. If it looks too good to be ________ it probably is.
4. Illegal downloading is the downloading of ________ to which you don’t have rights to.
5. You can put your computer at ________ if you download illegal media.
6. You can get a ________ record if you participate in illegal downloads
Lesson 13: Memorandum

Instruction: Complete the following crossword puzzle by filling in the missing words from the sentences and matching the word in the crossword puzzle.

1. Peer-to-peer downloading is **illegal**.
2. **Music** is an example of media.
3. If it looks too good to be **true** it probably is.
4. Illegal downloads is the downloading of **media** to which you don’t have rights to.
5. You can put your computer at **risk** if you download illegal media.
6. You can get a **criminal** record if you participate in illegal downloads.

```
  T
 S R I S K
 U I
 E

  M
 U

  M
 U

  I
 L

  L

  E
 E

  D
 G

  A
 L

  I
 N
 A
 L

  C R I M I N A L
  A
  L
```
### Overview:
Cyber bullying is the deliberate act by an individual or a group, through the use of information technology communication mediums such as social media, emails, instant messaging etc., to cause harm to another. With the increase of access to technology, cyber bullying has become a common trait among teenagers. The Internet allows a smokescreen behind which aggressors of cyber bullying can hide whilst bullying their victims.

Some victims are negatively influenced by cyber bullying which can have a significant effect on them, such as an increase feeling of sadness, loss of interest in activities and a lower self-esteem. This lesson will focus on cyber bullying in order to explore why it is wrong, what should be done if you are a victim and what will happen should you be the aggressor of cyber bullying.

This lesson is all about cyber bullying. It emphasises the importance of reporting cyber bullying to a parent or teacher.

<table>
<thead>
<tr>
<th>Learning Objectives:</th>
<th>Primary:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know how to handle cyber bullying should you ever become a victim.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secondary:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Know how to react to cyber bullies.</td>
</tr>
<tr>
<td>2. Examples of cyber bullying.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Materials:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video: Faux Paw Meets the First Lady: How to Handle Cyber bullying <a href="https://www.youtube.com/watch?v=RKi9FybL-Og">https://www.youtube.com/watch?v=RKi9FybL-Og</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Procedure:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Watch video</td>
</tr>
<tr>
<td>3. Reflect on video with class discussion</td>
</tr>
<tr>
<td>4. Explain main lesson concepts</td>
</tr>
<tr>
<td>5. Do class assessment to measure understanding and insight</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Discussion:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Questions for class discussion:</td>
</tr>
<tr>
<td>1. What examples of bullying can you mention out of the video?</td>
</tr>
<tr>
<td>2. What did Faux Paw do wrong after being bullied?</td>
</tr>
<tr>
<td>3. Did Faux Paw react in the right manner?</td>
</tr>
<tr>
<td>4. What should she have done?</td>
</tr>
<tr>
<td>5. To whom should you report cyber bullying?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assessment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worksheet: Find the words</td>
</tr>
</tbody>
</table>
Instruction: The following word search assignment contains examples of different types of cyber bullying. Find each word in the word search block.

STALKING - DEGRADATION - HUMILIATION - HARASSING - IMPERSONATING - FLAMING - WEBSITE - MESSAGING
Instruction: The following word search assignment contains examples of different types of cyber bullying. Find each word in the word search block.
Overview:
Protecting your personal information is becoming ever more important as more technologies become a part of our daily lives. It is very naïve to think that saving bank details and passwords on your local machine wouldn’t cause much damage, but the moment you connect to the Internet you run the risk of spyware and hackers possibly gaining access to such information. Lesson 15 places focus on online privacy. It’s not only about protecting your online information, but your computer as well. To keep your information private, only have people you know as friends on Facebook, change location based services settings to your personal needs, and protect your computer through updating security software.

Some terminology used the video:
- Location based services (LBS): A service allowing a website to track your geographical location based on where you are accessing the internet from.
- Peer-to-peer file sharing: Allows users to access media files such as books, music, movies, and games using a P2P software program (uTorrent) that searches for other connected computers on a P2P network to locate the desired content. Lately most of this content infringes on copyrights of the media and is downloaded illegally.

Learning Objectives:
Primary:
Comprehend the importance of keeping personal information private.

Secondary:
1. Understand privacy settings and safety measures
2. Know that updated computer security software is extremely important.

Materials:
Video: SafetyBratZLIVE! PSA -Protection Connection -Online Safety -Think Before You Click!
http://www.youtube.com/watch?v=vYIfnjgn_eY

Procedure:
1. Overview of Privacy.
2. Watch video.
3. Reflect on video with class discussion.
4. Explain main lesson concepts.
5. Do class assessment to measure understanding and insight.

Discussion:
Questions for class discussion:
1. What are some examples of information you should keep safe and private?
2. What is computer security software? (anti-virus/firewall)
3. How can information stored on your computer be compromised?
4. How can you prevent strangers from seeing what you share on the Internet? (Unfriend strangers/privacy settings)
5. Is it possible for websites to know where you are? How? (LBS)
6. Discuss why it is inappropriate to befriend a teacher on Facebook.

Assessment:
Worksheet: Match columns. Answers in order (top to bottom) – B;D;A;E;C
### Lesson 15: Assessment

*Instruction: Match the most suitable picture in Column B with the term in Column A*

<table>
<thead>
<tr>
<th>Column A</th>
<th>Column B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Based Services</td>
<td><img src="image1.png" alt="A" /></td>
</tr>
<tr>
<td>Untrusted Pop-up</td>
<td><img src="image2.png" alt="B" /></td>
</tr>
<tr>
<td>Computer Virus</td>
<td><img src="image3.png" alt="C" /></td>
</tr>
<tr>
<td>Don’t befriend strangers on Facebook</td>
<td><img src="image4.png" alt="D" /></td>
</tr>
<tr>
<td>Peer-to-peer file sharing program</td>
<td><img src="image5.png" alt="E" /></td>
</tr>
</tbody>
</table>
### Lesson 15: Memorandum

*Instruction: Match the most suitable picture in Column B with the term in Column A*

<table>
<thead>
<tr>
<th>Location Based Services</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Untrusted Pop-up</td>
<td>D</td>
</tr>
<tr>
<td>Computer Virus</td>
<td>A</td>
</tr>
<tr>
<td>Don’t befriend strangers on Facebook</td>
<td>E</td>
</tr>
<tr>
<td>Peer-to-peer file sharing program</td>
<td>C</td>
</tr>
</tbody>
</table>

A: Trojan horse
B: Untrusted pop-up alert
C: µTorrent icon
D: Untrusted pop-up
E: Online retail scam
Overview:
Cyber bullying is the deliberate act by an individual or a group, through the use of information technology communication mediums such as social media, emails, instant messaging etc., to cause harm to another. With the increase of access to technology, cyber bullying has become a common trait among teenagers. The Internet allows a smokescreen behind which aggressors of cyber bullying can hide whilst bullying their victims.

Some victims are negatively influenced by cyber bullying which can have a significant effect on them, such as an increase feeling of sadness, loss of interest in activities and a lower self-esteem. This lesson will focus on cyber bullying in order to explore why it is wrong, what should be done if you are a victim and what will happen should you be the aggressor of cyber bullying.

Lesson 16 is all about cyber bullying online. It emphasises the fact that teenagers use the Internet a lot. This lesson addresses how to react towards cyber bullies and makes know the fact that there might be consequences for perpetrators.

<table>
<thead>
<tr>
<th>Learning Objectives:</th>
<th>Primary:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Realise that talking online is the same as talking in real life, only mediums differ.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Secondary:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Know how to react towards cyber bullies.</td>
</tr>
<tr>
<td></td>
<td>2. Understand the possible consequences of being a bully.</td>
</tr>
</tbody>
</table>

| Materials: | Video: SafetyBratZLIVE! PSA - Stand Up To Cyber-Bullying - Think Before You Click! [http://www.youtube.com/watch?v=Hfi881lONSk](http://www.youtube.com/watch?v=Hfi881lONSk) |

|           | 2. Watch video. |
|           | 3. Reflect on video with class discussion. |
|           | 4. Explain main lesson concepts. |
|           | 5. Do class assessment to measure understanding and insight. |

| Discussion: | Questions for class discussion: |
|            | 1. Why is talking online the same as talking in real life? |
|            | 2. How should you react if you are being bullied online? |
|            | 3. What should you do if you see someone else being bullied? |
|            | 4. What can happen to you if you bully someone online? |
|            | 5. How should you treat other people online? |

| Assessment: | Worksheet: Letter |
Lesson 16: Assessment

Instruction: You have noticed for the past month that someone you don’t know have been making rude remarks on photos and saying mean things to your friend on Facebook and Twitter. You have noticed your friend is becoming very introverted and not themselves. Write a letter to your friend to help him/her feel better and give some advice as to what you think they should do.

__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________

Your friend

________________________
Lesson 16: Memorandum

Instruction: You have noticed for the past month that someone you don’t know have been making rude remarks on photos and saying mean things to your friend on Facebook and Twitter. You have noticed your friend becoming very introverted and not being themselves. Write a letter to your friend to help him/her feel better and give some advice as to what you think they should do.

For this assignment the instructor can use his/her own knowledge to judge whether the written letter is appropriate and whether the child has a good understanding of what cyber bullying is and what to do in a situation like this.
Overview:
Children of today have been branded as the “cyber generation”. They grow up and live with all
types of technologies and some parents sometimes do not hesitate in saying their children are
more tech-savvy than them. Children use these technologies to access social media to stay in
touch with their friends. They use it for sending messages, sharing photos or even funny videos.

The topic for Lesson 17 is “share with care” and it emphasises the need for children to know that
they need to take care when sharing content online. A video or photo you share with a friend
now might come back to haunt you in the future when applying to university or a job as more
recruiters use social media as a means of background checking possible employees. Information
you share might also fall into the hands of strangers. Many children accept friend requests from
people they don’t know, not knowing that this person has full access to everything they share. So
the message is: think before you share.

<table>
<thead>
<tr>
<th>Learning Objectives:</th>
<th>Primary:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Realise the importance of sharing with care.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secondary:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Know how to determine whether something is appropriate to share.</td>
</tr>
<tr>
<td>2. Understand future consequences of material you share now.</td>
</tr>
</tbody>
</table>

Materials:
Video: Safety BratZ LIVE! PSA - Share With Care - Online Safety Think Before You Click
http://www.youtube.com/watch?v=vijhpQxnQM

Procedure:
1. Overview of online sharing. Recap Lesson 16.
2. Watch video.
3. Reflect on video with class discussion.
4. Explain main lesson concepts.
5. Do class assessment to measure understanding and insight.

Discussion:
1. What would be inappropriate to share online?
2. How should you check whether something is appropriate to share?
3. Why can sharing inappropriate content affect you negatively in the future?
4. How would you feel if your parents read everything you post online?
5. Do you think privacy settings is enough to protect you information?

Assessment:
Worksheet: Status rating exercise
Lesson 17: Assessment

Instruction: Rate the following status updates as appropriate (YES) or inappropriate (NO). Discuss.

### Peter Couch
*September 16 near Summenstrad*

- **YES**: Took my dad's car out for a spin today! He doesn't know. Had a near miss experience with a bus, LOL, ahhh...

### Peter Couch
*September 16 near Summenstrad*

- **NO**: Had a very nice lunch with mom after school today! Burger was yummmmm! #ThanksMom

### Sara Thompson
*September 16 near Summenstrad*

- **NO**: CHILLING AT THE BEACH WITH MY NEW BIKINI...

### Sara Thompson
*September 16 near Summenstrad*

- **NO**: Had the worst test of my life... Who needs tests anyway? Tests are dumb and maths are for geeks!! Wish Mr. Cunningham would just drive into a tree so we never have to write a math test again... #AmIright?

### Peter Couch
*September 16 near Summenstrad*

- **YES**: This video of a guy being hit by a car is SO funny! Definitely need to watch this! LOL

### Sara Thompson
*September 16 near Summenstrad*

- **YES**: Had such a great day with my friends! Was an amazing experience. Would go help out at the animal shelter again any day! Wish more people would care for these abandoned pets... Someone interested in adopting??? Thanks Kayla for joining me :D
Lesson 17: Memorandum

*Instruction: Rate the following status updates as appropriate (YES) or inappropriate (NO).*

<table>
<thead>
<tr>
<th>Status Update</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Took my dad's car out for a spin today! :D He doesn't know. Had a near miss with a bus, LOL. sssh...</td>
<td>NO</td>
</tr>
<tr>
<td>Had a very nice lunch with mom after school today! Burger was yummyyy! #ThanksMom</td>
<td>YES</td>
</tr>
<tr>
<td>CHILLING AT THE BEACH WITH MY NEW BIKINI...</td>
<td>NO</td>
</tr>
<tr>
<td>Had the worst test of my life... Who needs tests anyway? Tests are dumb and maths are for geeks! Wish Mrs. Cunningham would just drive into a tree so we never have to write a maths test again... #AmIRight?</td>
<td>NO</td>
</tr>
<tr>
<td>This video of a guy being hit by a car is SO funny! Definitely need to watch this! LOL</td>
<td>NO</td>
</tr>
<tr>
<td>Had such a great day with my friends! Was an amazing experience. Would go help out at the animal shelter again any day! Wish more people would care for these abandoned pets :(. Someone interested in adopting??? Thanks Kayla for joining me :D</td>
<td>YES</td>
</tr>
</tbody>
</table>
**Lesson 18:**

**Online safety**

**Overview:**
As was seen in Lesson 17, taking care when sharing information, photos or videos online is very important. Privacy settings are not enough to protect our information from potential predators.

Lesson 18 substantiates Lesson 17. If children are not aware that sharing something online means they are availing it to the rest of the world, they might fall prey to strangers invading their privacy. The video for this lesson emphasises this issue. One wouldn’t feel good if people you do not know, know things about you. Children need to take due care to protect their online information. Some tips include:
- Having strong privacy settings.
- Only accepting people you know as friends.
- Abstaining from posting personal information online.

<table>
<thead>
<tr>
<th>Learning Objectives:</th>
<th>Primary:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Understand that what you share is available for the world to see.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Secondary:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Comprehend the dangers involved with having strangers see your information.</td>
</tr>
<tr>
<td></td>
<td>2. Know how to prevent your personal information from being publicly available.</td>
</tr>
</tbody>
</table>

**Materials:**
- Video: Everyone Knows Your Name - Online Safety Commercial
  [http://www.youtube.com/watch?v=dT1GvPQG904](http://www.youtube.com/watch?v=dT1GvPQG904)

**Procedure:**
1. Overview of online sharing. Recap Lesson 17.
2. Watch video.
3. Reflect on video with class discussion.
4. Explain main lesson concepts.
5. Do class assessment to measure understanding and insight.

**Discussion:**
Questions for class discussion:
1. Why is there so much emphasis on keeping information private?
2. Do you think having friends on Facebook that you have never met is safe?
3. What could happen if a criminal got hold of your personal information?
4. Would you be happy knowing that some old guy can possibly see your photos from the beach vacation?
5. How would you suggest keeping your information private?

**Assessment:**
- Worksheet: Quiz
Lesson 17: Assessment

Instruction: Circle the most appropriate answer to the following questions:

1. If I am using privacy settings and only letting my friends see my profile, nothing can leak out.
   a. True
   b. False

2. If you deactivate your Facebook account, the information is no longer available.
   a. True
   b. False

3. University recruiters, admissions people and potential employers often look at an applicant’s social networking profile.
   a. True
   b. False

4. It is safe to give your school name over the Internet.
   a. True
   b. False

5. If someone online tells you they are in 8th grade and their name is Thabo, they are probably how old?
   a. 12
   b. 14
   c. You won’t know

6. You have been talking to a person on the Internet for a long time, and they want to meet, which is okay to do?
   a. Meet them, as long as you bring a friend.
   b. Meet in a crowded, public place.
   c. Ask your parent or guardian first and have them go with you.

7. You are talking to someone online and they know some of the same people you know. Since they have many of the same friends as you, is it acceptable to give them your phone number if they ask?
   a. Yes
   b. No

8. It is okay to send someone online your picture when:
   a. They send you theirs first
   b. You send them an old picture
   c. You don’t send
Lesson 18: Memorandum

Instruction: Circle the most appropriate answer to the following questions:

1. If I am using privacy settings and only letting my friends see my profile, nothing can leak out.
   a. True
   b. False

2. If you deactivate your Facebook account, the information is no longer available.
   a. True
   b. False

3. University recruiters, admissions people and potential employers often look at an applicant’s social networking profile.
   a. True
   b. False

4. It is safe to give your school name over the internet.
   a. True
   b. False

5. If someone online tells you they are in 8th grade and their name is Thabo, they are probably how old?
   a. 12
   b. 14
   c. You won’t know

6. You have been talking to a person on the internet for a long time, and they want to meet, which is okay to do?
   a. Meet them, as long as you bring a friend.
   b. Meet in a crowded, public place.
   c. Ask your parent or guardian first and have them go with you.

7. You are talking to someone online, and they know some of the same people you know. Since they have many of the same friends as you, is it ok to give them your phone number if they ask?
   a. Yes
   b. No

8. It is okay to send someone online your picture when:
   a. They send you theirs first
   b. You send them an old picture
   c. You don’t send
## Overview:
Social networking websites provide services to people to connect with others to share things like photos, activities, interests etc. Examples of social networking websites are Facebook, Twitter and Myspace. The risk when using these websites have increased dramatically since it has become more popular and for many people a part of life. Many cyber criminals, such as hackers and identity thieves, have seen an opportunity to gather private information about others through social networking sites to use it for malicious intent.

Ways to avoid becoming a victim:
- Don’t share private information on social networking sites.
- It is recommended not share information that can be used to harm your reputation.
- Don’t accept friend request from people you don’t know.
- Children’s parents/guardians should be aware of what information their children share online.

This lesson will emphasise the fact that children should take due care when sharing information or media on social networking websites.

## Learning Objectives:

<table>
<thead>
<tr>
<th>Primary</th>
<th>Understand the importance of not sharing private information and media online.</th>
</tr>
</thead>
</table>
| Secondary | 1. Be able to identify what information and media can pose a danger when shared.  
2. Knowing what the consequences of sharing private information and media are. |

## Materials:
- Video: NetSmartz.org Social Networking TIPS  
  [https://www.youtube.com/watch?v=Esj-PBmXjCU](https://www.youtube.com/watch?v=Esj-PBmXjCU)

## Procedure:
1. Overview of safe social networking.  
2. Watch video.  
3. Reflect on video with class discussion.  
4. Explain main lesson concepts.  
5. Do class assessment to measure understanding and insight.

## Discussion:
Questions for class discussion:
1. What is a social networking website? (Use examples)  
2. What information is safe to share online?  
3. What information should not be shared online?  
4. Why should your online profile be private?  
5. Who may you accept as you friend when you receive a friend request?  
6. What can the consequences be if you share private information and media

## Assessment:
- Worksheet: Multiple choice questions and rating table
Lesson 19: Assessment

Instruction: Circle the correct answer to the following questions:

1. What is an example of a social networking site?
   a. WeChat
   b. Facebook
   c. WhatsApp
   d. Google

2. What is usually posted on social networking sites (Choose 2)?
   a. Life events
   b. Documents
   c. Music
   d. Photos

3. In which menu do you usually set your profile as private?
   a. General settings
   b. Security settings
   c. Privacy settings
   d. Account settings

4. If you receive a friend request from someone you don’t know, what should you do?
   a. Accept invite
   b. Ignore the invite
   c. Ask parents
   d. Both b and c

Instruction: Mark the following posts as either safe or unsafe to post online:

<table>
<thead>
<tr>
<th>Post</th>
<th>Safe</th>
<th>Unsafe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photos of you and your friends at the beach.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Posting about a new game you bought and how cool it is.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A post that you feel is okay, but your parents/guardians might feel different.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>You post your cell phone number so that your friends have your contact number.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Doing regular check in’s on Facebook to show friends where you are.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A post with your friends’ party location.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A photo with family members.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Make a status about how great your friends’ party was.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lesson 19: Memorandum

Instruction: Circle the correct answer to the following questions:

5. What is an example of a social networking site?
   a. WeChat
   b. Facebook
   c. WhatsApp
   d. Google

6. What is usually posted on social networking sites (Choose 2)?
   a. Life events
   b. Documents
   c. Music
   d. Photos

7. In which menu do you usually set your profile as private?
   a. General settings
   b. Security settings
   c. Privacy settings
   d. Account settings

8. If you receive a friend request from someone you don’t know what should you do?
   a. Accept invite
   b. Ignore the invite
   c. Ask parents
   d. Both b and c

Instruction: Mark the following post as either safe or unsafe to post online:

<table>
<thead>
<tr>
<th>Post</th>
<th>Safe</th>
<th>Unsafe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photos of you and your friends at the beach</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Posting about a new game you bought and how cool it is</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>A post that you feel is okay, but your parents/guardians might feel different</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>A post with your friends’ party location</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>A photo with family members</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Make a status about how great your friends’ party was</td>
<td></td>
<td>*</td>
</tr>
</tbody>
</table>
Overview:
A lot of information is posted online these days. This creates some concern as a lot of information is private or confidential and can be used for malicious purposes should it fall into the wrong hands. Private information can also be shared amongst others online in the form of gossiping resulting in embarrassment or anger of the individual or group. It is the responsibility of each individual to ensure that their information stay private and cannot be accessed by others who should not have access to it. The safest way to do this is not to post any private or confidential information online.

Many people enjoy posting their life events and experiences on their blogs or social networking websites such as Facebook. They should ensure that no private information gets posted, such as their location or address. One should minimise details identifying you or your whereabouts. Also, one should be cautious of sharing private information with others through instant messaging as this can have the same consequences.

In this lesson the children will learn not to share their private information online or through instant messaging.

Learning Objectives:
Primary:
Knowledge of sharing private information online.

Secondary:
1. Understand what private information is.
2. Identify the consequences if private information is shared.

Materials:
Video: Netsmartz\NSTEENS Video on Internet Privacy
https://www.youtube.com/watch?v=9bhHaVxo3i0

Procedure:
2. Watch video.
3. Reflect on video with class discussion.
4. Explain main lesson concepts.
5. Do class assessment to measure understanding and insight.

Discussion:
Questions for class discussion:
1. What is examples of private information?
2. Give examples of what information can be shared online?
3. From the video what did Alie do wrong?
4. What is gossiping? (refer to video as example)
5. What are some consequences if you share private information online

Assessment:
Worksheet: Short questions
Lesson 20: Assessment

Instruction: Answer the following questions

1. Jerry just joined Facebook, but he is unsure about what he can post. Explain to Jerry what is meant by private information and give him examples?

_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________

2. Tell Jerry of some of the things that can happen if he post private information online?

_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________

3. Jerry asks you how do people gossip online?

_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________

4. Tell Jerry why he should not take part in gossiping?

_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________

5. Jerry has one last question for you. He has a crush on a girl in his class. He wants to post his feelings for her online. May Jerry do this and why do you think so?

_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
Lesson 20: Memorandum

Instruction: Answer the following questions

1. Jerry just joined Facebook, but he is unsure about what he can post. Explain to Jerry what is meant by private information and give him examples?

*Private information is personal information that should not be in the hands of potential criminals. Posting your home address, cell phone number or school name on Facebook is not safe.*

2. Tell Jerry of some of the things that can happen if he posts private information online?

*It can fall into the hands of people that use it for malicious intent. Criminals could break into your house if they know your address or even harass you if they get your number.*

3. Jerry asks you how do people gossip online?

*People use social media websites and Instant Messaging applications like BBM and WhatsApp to spread rumours and talk about people behind their backs.*

4. Tell Jerry why he should not take part in gossiping?

*It is rude to gossip, you hurt other people’s feelings and sometimes a gossip might lead to something worse like a false rumour that could have bad effects on someone.*

5. Jerry has one last question for you. He has a crush on a girl in his class. He wants to post his feelings for her online. May Jerry do this and why do you think so?

*Jerry is entitled to do so, but it is very inappropriate and not the right thing to do.*
## Lesson 21:
### Cyber Bullying

**Overview:**
Cyber bullying is the same as traditional bullying the only difference being the use of digital technologies. The victim gets either humiliated, embarrassed, threatened or tormented over digital technologies such as instant messaging or social media. It has become prominent amongst children and teens. The old saying “sticks and stones” don’t hold anymore as cyber bullying has made many left feeling emotional and in extreme cases some has committed suicide. This has raised awareness of cyber bullying in a fight to stop it.

People who cyber bully do it for entertainment, power, revenge or stupidity. Many is not even aware that they cyber bully. Victims of cyber bullying should not respond to it and tell a trusted adult. The harasser should be blocked, but first save all the communication as evidence. If someone sees a friend being cyber bullied, the victim should be supported and complimented.

In this lesson cyber bullying will be explained to the children and they will be taught about what should be done when becoming a victim of it and also to support one another in a fight against cyber bullying.

<table>
<thead>
<tr>
<th>Learning Objectives:</th>
<th>Primary: Knowledge of what cyber bullying is.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secondary:</td>
</tr>
<tr>
<td></td>
<td>1. Identify when you’re getting cyber bullied.</td>
</tr>
<tr>
<td></td>
<td>2. What to do when you’re a victim of cyber bullying.</td>
</tr>
</tbody>
</table>

| Materials: | Video: NetSmartz.org on Cyber bullying [https://www.youtube.com/watch?v=xGKmITtZnSk](https://www.youtube.com/watch?v=xGKmITtZnSk) |

| Procedure: | 1. Overview of cyber bullying. Recap Lesson 20 |
|            | 2. Watch video. |
|            | 3. Reflect on video with class discussion. |
|            | 4. Explain main lesson concepts. |
|            | 5. Do class assessment to measure understanding and insight. |

| Discussion: | Questions for class discussion: |
|            | 1. What does it mean when you get cyber bullied? |
|            | 2. Why do people cyber bully? |
|            | 3. What should you do when you get cyber bullied? |
|            | 4. Why should you save the evidence? |
|            | 5. When you see a friend getting cyber bullied what should you do? |

| Assessment: | Worksheet: Questions |
Lesson 21: Assessment

Instruction: Answer the following questions

1. What is the difference between bullying and cyber bullying?
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________

2. Why do people cyber bully?
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________

3. Should you feel embarrassed, threatened or humiliated when you get cyber bullied and why do think so?
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________

4. When you see your friend getting cyber bullied what should you do?
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________

5. How to you think can awareness be raised for cyber bullying?
_______________________________________________________________________________
_______________________________________________________________________________
_______________________________________________________________________________
Lesson 21: Memorandum

Instruction: Answer the following questions

1. What is the difference between bullying and cyber bullying?

   Cyber bullying is the same as normal bullying the only difference is that it occurs over electronic mediums and is non-physical

2. Why do people cyber bully?

   A lot of people commit cyber bullying out of fun or as a joke, but they do not realise what effect this has on the victim. You also get people who bully on purpose to cause harm to someone for a specific reason.

3. Should you feel embarrassed, threatened or humiliated when you get cyber bullied and why do you think so?

   No, one should not be cyber bullied at all, but if you become a victim this is some of the feelings one would encounter.

4. When you see your friend getting cyber bullied what should you do?

   In a scenario like this you should not be afraid to stand up for your friend and help him. Tell your parents or a teacher.

5. How to you think can awareness be raised for cyber bullying?

   *Mention anything like posters or presentations etc.*
# Lesson 22:

**Online posting can haunt you in the future**

## Overview:

This lesson strongly relates to lesson 19 and 20. Posting private information online is not the only thing that one should be careful of. Some information that you or anyone else post about you online may influence your reputation. For example, employers these days do an online look up of a person who applied for a work position to determine the history and personality of the person. Posting something now that might seem fine now to post, might have an influence in your future. The problem is that there might be some information of you online that you will never be able to remove. So the best way to avoid online post that might haunt you in the future is not to post them at all. If already posted, consideration should be taken to make an effort to remove it immediately.

In this lesson the children will be taught about the consequences of posting something now that might influence them in the future.

## Learning Objectives:

<table>
<thead>
<tr>
<th>Primary:</th>
<th>Understand how posting something online now can have an influence in your future.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary:</td>
<td>1. Identify what is safe to post online that will not have an influence in your future.</td>
</tr>
<tr>
<td></td>
<td>2. Understand the consequences when you post something online that will have an influence in your future.</td>
</tr>
</tbody>
</table>

## Materials:

<table>
<thead>
<tr>
<th>Video: Profile Penalty 2000k</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://www.youtube.com/watch?v=V3DIVkOAPVQ">https://www.youtube.com/watch?v=V3DIVkOAPVQ</a></td>
</tr>
</tbody>
</table>

## Procedure:

<table>
<thead>
<tr>
<th>1. Overview of online posting that can influence your future. Recap Lesson 21.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Watch video.</td>
</tr>
<tr>
<td>3. Reflect on video with class discussion.</td>
</tr>
<tr>
<td>4. Explain main lesson concepts.</td>
</tr>
<tr>
<td>5. Do class assessment to measure understanding and insight.</td>
</tr>
</tbody>
</table>

## Discussion:

<table>
<thead>
<tr>
<th>Questions for class discussion:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What is meant by safe online posting?</td>
</tr>
<tr>
<td>2. How do you know if something is safe to post online?</td>
</tr>
<tr>
<td>3. Is it okay to post a video online where you break a rule?</td>
</tr>
<tr>
<td>4. What is the best thing to do if you are unsure if you can post something online?</td>
</tr>
<tr>
<td>5. What can be influenced in your future by posting something now?</td>
</tr>
</tbody>
</table>

## Assessment:

<table>
<thead>
<tr>
<th>Worksheet: Fill in the missing words then in the crossword puzzle</th>
</tr>
</thead>
</table>
Lesson 22: Assessment

Instruction: Fill in the missing words in the crossword puzzle:

1. Posting private information may influence your __________.
2. _______ networking websites are examples where you should be cautious to post private information.
3. People can also read your online ______, so one should be careful of what you write.
4. When you are unsure if a post is safe to put online, you should ask a ______ adult.
5. _______ do online searches of you when you apply for a job.
6. Online posts also include ______ such as photos.
7. There might be a chance that you will never be able to ______ old posts.
8. Posting statuses, photos or videos where you break rules might ______ your future
Lesson 22: Memorandum

*Instruction: Fill in the missing words in the crossword puzzle:*

1. Posting statuses, photos or videos where you break rules might **influence** your future.
2. Posting private information may influence your **future**.
3. When you are unsure if a post is safe to put online you should ask a **trusted** adult.
4. People can also read your online **blog** so one should be careful of what you write.
5. **Social** networking websites is examples where you should be cautious to post private information.
6. Online posts also include **Media** such as photos.
7. **Employees** do online searches of you when you apply for a job.
8. There might be a chance that you will never be able to **remove** old posts.

```
  I
N
F
  B L O G
  U
  E M P L O Y E E S
  N c D T
  C I I E
  R E M O V E A A D
  L
```

**Lesson 23:**

**Be careful of online friends**

**Overview:**
Chatting online has become very common amongst friends and even strangers. There are many methods to meet new people online through social media. The risk of this is that the person on the other side, the stranger, might not be who they say they are. They can create a fake profile and make you think you have personal interest in common. The stranger will then try to gather personal information to use in a malicious attack or even worse, try to meet offline with the victim. This can have serious consequences such as robbing of the victims personal items or raping. When chatting to online strangers, children should be careful not to give personal details out and when asked to meet offline the child should say no or consult with his/her parents. When the stranger is a friend-of-a-friend, the situation might be different and an offline meeting might be arranged, but the child should still consult his/her parents before meeting offline.

In this lesson the children will be taught of the dangers of meeting online friends’ offline and convince them not to do it.

**Learning Objectives:**

| Primary: | Knowledge of online friends and meeting them offline. |
| Secondary: | 1. To understand what an online friend is.  
2. Risk involved of communication of online strangers and meeting them offline. |

**Materials:**

| Video: Friend or Fake  
https://www.youtube.com/watch?v=y4nyluaXoFY |

**Procedure:**

1. Overview of online friends. Recap Lesson 22.  
2. Watch video.  
3. Reflect on video with class discussion.  
4. Explain main lesson concepts.  
5. Do class assessment to measure understanding and insight.

**Discussion:**

| Questions for class discussion:  
1. What is an online friend?  
2. Can an online friend be who he/she claims to be?  
3. Why would an online friend fake their identity?  
4. May you meet online friends’ offline?  
5. What are the risk of meeting an online friend offline?  
6. What should you always do when you’re in doubt and why? |

**Assessment:**

| Worksheet: Fill in the missing words then in the crossword puzzle |
Lesson 23: Assessment

Instruction: Fill in the missing words in the crossword puzzle

1. Online friends are friends that you only know ________.
2. An online friend may not be ________.
3. Hackers and identity thieves create ________ profiles to gather information from victims.
4. Only people that you ________ should be on your friend list.
5. An online friend is always a ________ no matter how well you know the person online.
6. You should never meet an online friend ________ without asking your parents/guardians.
7. An online friend may _____ you when you meet offline.
8. Remember, if your online friend seems too _____ to be true, he/she probably is.
Lesson 23: Memorandum

*Instruction: Fill in the missing words in the crossword puzzle*

1. Online friends are friends that you know **online**.
2. Hackers and identity thieves create **fake** profiles to gather information from victims.
3. Remember, if your online friend seems too **good** to be true it properly is.
4. An online friend may **rob** you when you meet offline.
5. Only people that you **know** should be on your friend list.
6. You should never meet an online friend **offline** without asking your parents/guardians.
7. An online friend is always a **threat** no matter how well you think you know the person online.
8. An online friend may not be **real**.

![Crossword Puzzle]

```
   O       F       A       N
   E       E       L
   R       T       O
   I       K

   1. Online
   2. Fake
   3. Good
   4. Rob
   5. Know
   6. Offline
   7. Threat
   8. Real
```
**Lesson 24:**

Sexting

**Overview:**
Sexting is defined as the act of sending sexually explicit messages, primarily between mobile phones. The term was first popularized in the early 21st century, and is an amalgamation of sex and texting, where the latter is meant in the wide sense of sending a text possibly with images. Sexting is a result of advances in technology enabling new forms of social interaction. Messages with sexual content can be exchanged from phones, emails, or social media websites. Newer technology allows sending pictures and videos. A social danger with sexting is that material can be very easily and widely propagated, over which the originator has no control.

Lesson 24 deals with sexting to find out what it is, why it is wrong and the risks it carries. With applications such as WhatsApp and BBM allowing instant sharing of photos and videos, the act of sexting has become easier to accomplish. What teens do not realize is that sending material as private as this to someone you think you trust can have major consequences. You are not in control of what happens to that material and who sees it after you have sent it.

**Learning Objectives:**

<table>
<thead>
<tr>
<th>Primary</th>
<th>Understand the concept of sexting.</th>
</tr>
</thead>
</table>
| Secondary | 1. Know what consequences sexting may have.  
2. Comprehend why it is inappropriate | |

**Materials:**

| Video: Sexting safety tips (3 of 3): Don't incite it!  
http://www.youtube.com/watch?v=AL5Y6rJwTuQ |

**Procedure:**

2. Watch video.  
3. Reflect on video with class discussion  
4. Explain main lesson concepts  
5. Do class assessment to measure understanding and insight

**Discussion:**

Questions for class discussion:

1. Who can give an explanation of what sexting is?  
2. How does it work?  
3. Do you think sexting is appropriate for children?  
4. What risks are involved when you sext?  
5. What can happen if you are caught sexting?

**Assessment:**

Worksheet: Word search assignment
Lesson 24: Assessment

Instruction: Fill in the missing words in the following paragraph then find the words in the word search puzzle.

Sexting is the act of sending ______________ explicit messages, primarily using __________. Newer technologies allow the sending of _________ and _______ at almost no cost, which makes it easier for teens to sext. What most teens do not know is that sexting is against the _______. You can get into a lot of _________ if you get caught. Something that would be more ___________ to you is if a photo or video you sent to someone _________ out and is seen by many of your school _________.

WORD SEARCH PUZZLE:

G D Y C E L L P H O N E S Z G
E L B U O R T E T S B M M F B
H Y T B W H M S H C O V B W H
M G H J G S X I Q P W E U G D
Z U P O N L F I T G A R D B J
Y E W U I S E X U A L L Y I W
M U L S S V V X X S W S R P V
V C O R S C C G A N P O I O Q
Z J E E A N C L Z E M T N J A
H J A E R L W L N Y R O C F T
O C G P R Z E G A B I H I E D
Y E I E A S F A E G M P O X V
O X U O B J J W K L A L O E V
J X U O M M L P G S Q X W M Y
O H X Q E B W Y N X Q J H X M
Lesson 24: Memorandum

Instruction: Fill in the missing words in the following paragraph then find the words in the word search puzzle.

Sexting is the act of sending sexually explicit messages, primarily using cellphones. Newer technologies allow the sending of photos and videos at almost no cost, which makes it easier for teens to sext. What most teens do not know is that sexting is against the law. You can get into a lot of trouble if you get caught. Something that would be more embarrassing to you is if a photo or video you sent to someone leaks out and is seen by many of your school peers.