Analysis of a South African cyber-security awareness campaign for schools using interdisciplinary communications frameworks.

by

Claudette Leppan (s207064641)

Dissertation submitted in fulfilment
of the requirements
for the degree

MAGISTER ARTIUM

in

MEDIA STUDIES

To be awarded at
NELSON MANDELA METROPOLITAN UNIVERSITY (NMMU)
April 2017

Supervisor: Prof. Johan van Niekerk
Co-supervisor: Dr. Belinda du Plooy

DECLARATION

I, Claudette Leppan (s207064641), hereby declare that the dissertation for MA: Media Studies to be awarded is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

SIGNATURE: C Leppan

DATE: 28/02/2017

ABSTRACT

To provide structure to cyber awareness and educational initiatives in South Africa, Kortjan and Von Solms (2014) developed a five-layer cyber-security awareness and education framework. The purpose of the dissertation is to determine how the framework layers can be refined through the integration of communication theory, with the intention to contribute towards the practical implications of the framework. The study is approached qualitatively and uses a case study for argumentation to illustrate how the existing framework can be further developed. Drawing on several comprehensive campaign planning models, the dissertation illustrates that not all important campaign planning elements are currently included in the existing framework. Proposed changes in the preparation layer include incorporating a situational and target audience analysis, determining resources allocated for the campaign, and formulating a communication strategy. Proposed changes in the delivery layer of the framework are concerned with the implementation, monitoring and adjustment, as well as reporting of campaign successes and challenges. The dissertation builds on, and adds to, the growing literature on the development of campaigns for cyber-security awareness and education aimed at children.

Keywords: Cyber-safety, cyber-safety awareness, campaign planning

ACKNOWLEDGEMENTS

To my supervisors and mentors, Prof Johan van Niekerk and Dr. Belinda du Plooy, thank you for your motivation, guidance and assistance in the research journey. “Sometimes the questions are complicated, and the answers are simple.” (Dr. Seuss)

To Ronald, thank you for all your love and support, for assisting in the technical editing of the document and for making coffee during midnight work sessions. “All that a husband or wife really wants is to be pitied a little, praised a little, and appreciated a little.” (Oliver Goldsmith)

To my parents, Deon and Tersia, thank you for your support and for sending all the sweet treats to go with the coffee. “The most beautiful thing in the world is to see your parents smile and to know that you are the reason behind the smile.”

To Zani, thank you for your love and support. “A sister can be seen as someone who is both ourselves and very much not ourselves – a special kind of double”. (Toni Morrison)

To Viwe, ungu dadewam komnye umamawam. Kwaye, uyinto yonke kum. Thank you for your love and support, especially when I felt overwhelmed with balancing my work and study commitments. “I may not have gone where I intended to go, but I think I have ended up where I needed to be.” (Douglas Adams)

To Beulah and Kelli, thank you for assisting me to cross-check my references when my referencing software failed just before the submission deadline. “Friendship isn’t about whom you have known the longest, it’s about who came, and never left your side.”

To Vicky, thank you for the language editing and suggestions to improve my work.

To Hoessain, thank you for your words of encouragement when I needed it most. “If you really believe in what you are doing, work hard, take nothing personally and if something blocks one route, find another. Never give up.” (Laurie Notaro)

Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AIDA	Attention, interest, desire, action
C3	Cyber-ethics, Cyber-safety, Cyber-security
CRICS	Centre for Research in Information and Cyber Security
CSA	Cyber-Safety Awareness
CSAW	Cyber-Security Awareness Workbook
DBE	Department of Basic Education
DHET	Department of Higher Education and Training
ICT	Information and Communication Technology
IICTA	Institute for Information and Communication Technology Advancement
ICT4D	Information and Communication Technology for Development
ICT4E	Information and Communication Technology for Education
IT	Information Technology
KPIs	Key Performance Indicators
MMORPG	Massive Multiplayer Online Role-Playing Games
NMMU	Nelson Mandela Metropolitan University
NCPF	South African National Cyber Safety Policy Framework
NSSF	The National School Safety Framework
PR	Public Relations
UJ	University of Johannesburg
UNISA	University of South Africa
SACSAA	South African Cyber Safety Academic Alliance
SMARTA	Specific, Measurable, Attainable, Realistic, Time-bound, Adjustable

CHAPTER 1 INTRODUCTION

“I don't see how *s*he can ever finish, if *s*he doesn't begin.”

(Lewis Carroll, Alice's Adventures in Wonderland)

<table>
<tr><td colspan="3">**Entry vignette**
Abstract</td></tr>
<tr><td colspan="3">**Introduction to case and context**
Chapter one: Introduction
Research question:
What are the elements required for the preparation and delivery of a cyber-safety awareness campaign?</td></tr>
<tr><td colspan="3">Chapter two: Research methodology</td></tr>
<tr><td rowspan="3">**Research objective I.**
To identify, using existing literature, the essential elements required for conducting a cyber-safety awareness campaign in South Africa.</td><td colspan="2">**Description of case and context**</td></tr>
<tr><td>Chapter three: Cyber-safety in South Africa</td><td>Chapter four: Campaign planning</td></tr>
<tr><td>*Information Technology perspective*</td><td>*Communication Science perspective*</td></tr>
<tr><td>**Research objective II.**
To describe an existing South African cyber-safety awareness campaign aimed at schools, which forms the single case study;</td><td rowspan="2" colspan="2">**Development and detail about selected of issues**
Chapter five:
SACSAA campaign</td></tr>
<tr><td>**Research objective III.**
To compare the case study with the identified elements, and to determine whether there are any application gaps and areas for improvement;</td></tr>
<tr><td>**Research objective IV.**
To make recommendations for improved and integrated strategies for cyber awareness campaigns in South Africa.</td><td colspan="2">**Lessons learnt and closing vignette**
Chapter six:
Conclusion
Findings and recommendations</td></tr>
</table>

1.1 Introduction

The term ‘cyberspace’ is not novel; it has been used since the 1980’s to refer to new technologies and devices which enable users to access the Internet and connect with others (Strate, 1999). Although the online world has been in existence for quite some time and Internet users have increased (Stork, Calandro & Gillwald, 2013), all users are not necessarily equipped with the knowledge required to deal with the ever-changing dangers online (Quigley, Burns & Stallard, 2015). As more people gain access to technology and the Internet, the need to teach users to navigate the online world responsibly and safely has become more urgent (Deibert, 2012).

To address online dangers, Gcaza, Von Solms and Van Vuuren (2015) explored the creation of a national cyber-security culture. Achieving the goal of creating a cyber-safe culture, requires ongoing initiatives to educate and remind users about online risks (Rantos, Fysarakis & Manifavas, 2012). Initiatives should be coordinated and therefore, Kortjan and Von Solms (2014) developed a conceptual framework for cyber-security awareness and education campaigns in South Africa. Developing effective campaigns which lead to behaviour change (Bada & Sasse, 2014), finds its roots in the field of Communication Science (James, 2011; Werder, 2015). The study of communication incorporates different theoretical contributions from humanities, sociology, psychology, philosophy, and literature, with the intent of exploring the verbal and non-verbal exchange of information in different settings (Pooley, 2016). The link between communication theory and Information Technology (IT) has been established (Hammick & Lee, 2014), but the integration of communication theory for cyber-security campaign planning can be further explored to contribute to the overall effectiveness of campaign initiatives. Therefore, for the purpose of this study, the framework developed by Kortjan and Von Solms (2014) will be analysed from a Communication Science perspective.

To motivate for the analysis of the framework from a Communication Science perspective, chapter one provides an overview of cyber-security and communication theory used for campaign planning. The framework developed by Kortjan and Von Solms (2014) is discussed briefly to indicate areas of concern which can be addressed by communication theory. These areas of concern forms the rationale and purpose of the study which is addressed through the research question and research objectives outlined in chapter one. An overview of the research design used for the study, as well as the assumptions, limitations and significance of the research, is introduced in the chapter. The process followed for the study is presented in table format to orientate the reader, followed by a list of the key terminology used throughout the study. Chapter one concludes with an overview of the main ideas discussed in the first section of the dissertation.

1.2 Cyber-security

There is ongoing research to improve cyber-security systems (Bendovschi, 2015; Julisch, 2013; Maskun, Manuputty, Noor & Sumardi, 2013) and to implement enhanced cyber-security technology (Such, Gouglidis, Knowles, Misra & Rashidet, 2016; Skopik, Settanni & Fielder, 2016). However, the continuous development of cyber-security systems has led some attackers to shift the focus from computer systems to targeting human users directly (Al-Khateeb & Epiphaniou, 2016; Henshel, Cains, Hoffman & Kelley, 2015; Pfleeger & Caputo, 2012). Organisations provide information security training to employees to protect their information systems (Gurnani, Pandey & Kant Rai, 2014), but Von Solms and Van Niekerk (2013) argue that the focus should be on cyber-security training as humans can also fall victim to online dangers.

Although there has been an increase in cyber-related legislation to protect users from cyber-attacks (Davis, 2012; Menon & Siew, 2012), humans unintentionally create susceptibilities for cyber-security systems (Ashenden, 2008). Negligent behaviour (Alavi, Islam, & Mouratidis, 2016) and a limited awareness of risks (Reid & Van Niekerk, 2014; Slusky & Partow-Navid, 2012) are key elements creating vulnerabilities for information security systems.

Globalisation (McCrohan, Engel & Harvey, 2010) and the rapid development of technology (Özgür, 2016) leads to increased cyber risks (Tikk, 2011; Wong, 2010). These risks highlight the need for users to be informed about dangerous online behaviour (Ey & Cupit, 2011; Saridakis, Benson, Ezingeard & Tennakoon, 2016). The lack of cyber-safety awareness is one of the major cyber-security concerns in South Africa (Kritzinger, 2014; Swart, Irwin & Grobler, 2014). One way of informing users about the risks associated with the use of IT is the development of awareness and educational campaigns (Lebek, Uffen, Neumann, Hohler & Breitner, 2014). Awareness of cyber risks is believed to assist users in making more informed decisions (Slonje, Smith & Frisén, 2013). Various researchers have proposed interventions for cyber awareness and education (Amankwa, Look & Kritzinger, 2015; Dlamini, Taute & Radebe, 2011;

Labuschagne, Burke, Veerasamy & Eloff, 2011). Creating a dialogue regarding cyber-security issues, ensuring participation of all stakeholders (Martin & Rice, 2011; Ong, 2015; Shillair, Cotten, Tsai, Alhabash, LaRose & Rifon, 2015) and reflecting on cyber-security practices are strategies proposed to manage cyber-security effectively (Albrechtsen & Hovden, 2010).

Cyber awareness is an essential aspect of information security (Aloul, 2012). The purpose of information security awareness initiatives is to direct the attention of the target audience to cyber-security issues, while cyber-security education focuses on providing insight into cyber-security issues (Amankwa, Loock & Kritzinger, 2014). Pusey and Sadera (2011) distinguishes between cyber-security as computer systems implemented to protect computer hardware and software against malware; and cyber-safety which focuses on teaching users to act responsibly online.

The purpose of cyber awareness and education campaigns is to ensure that users understand best practices and protect themselves online (Abawajy, 2014). Vulnerable groups such as children are important target audiences for campaigns (Ktoridou, Eteokleous & Zahariadou, 2012) as they can engage in risky behaviour (Aiken, Mc Mahon, Haughton, O'Neill & O'Carroll, 2015). Children can fall victim to online sexual harassment, pornography, cyberbullying and technology addiction (Tomczyk & Kopecký, 2016).

Not all children have access to Information and Communication Technology (ICT) infrastructure in South Africa (Kritzinger, 2014; Van Niekerk & Blignaut, 2014), but mobile phones are used to access the Internet (Unicef, 2012). Mobile devices, however, are often not monitored by children's guardians and teachers (Jobi & Kritzinger, 2014). Although the Internet holds several advantages for use in education, schools find it challenging to monitor online behaviour (Mark & Ratliffe, 2011), and too much Internet exposure causes anxiety, depression and impulsive behaviour in learners (Kim & Kim, 2015).

There are existing initiatives in South Africa to inform and educate children about cyber-safety issues and risks. Organisations in the business sector develop online platforms and resources for users such as parents and educators (Kritzinger, 2016). Higher Education Institutions develop campaigns and community projects such as PumaScope, developed by the University of Pretoria, and initiatives to inform rural communities such as the Council for Scientific Industrial Research (Grobler, Dlamini, Ngobeni & Labuschagne, 2011) and the University of Venda projects (Dlamini & Modise, 2012). Although short-term initiatives have been effective (Reid & Van Niekerk, 2014b), campaigns tend to take place in different parts of South Africa and tend to be small in size (Dlamini & Modise, 2012), which highlights the need for an integrated national approach (Kortjan & Von Solms, 2014).

1.3 South African schools

Education in South Africa is managed by the Department of Basic Education (DBE) and the Department of Higher Education and Training (DHET) (Government of South Africa, 2016). While schooling is compulsory for learners aged seven to fifteen, enrollment at a public or independent school for Grade R is possible at the age of five (Government of South Africa, 2016). The DBE manages the curriculum of Grade R to Grade Seven learners, who attend primary school, as well as the Grade Eight to Grade Twelve pupils who attend high school. Public schools are controlled and funded by the South African government, while independent schools, though registered with the DBE, are governed and funded privately (Amod, Vorster & Lazarus, 2013; Government of South Africa, 2016).

Travelling distances and financial implications influence whether a learner will attend schooling in an urban, suburban, township or rural area (De Kadt, Norris, Fleisch, Richter & Alvanides, 2014). Schools located in residential areas are often referred to as good schools (Donaldson, Mehlomakhulu, Darkey, Dyssel & Siyongwana, 2013) and are attended by more affluent learners (Bayat, Louw & Rena, 2014). Township schools are located in informal settlement areas, associated with high unemployment rates (Altman, Schöer & Rama, 2013) and poverty (Mestry & Ndhlovu, 2014; Ramnarain, 2014). Rural schools are located in underdeveloped countryside areas which, at times, are without essential resources or services (Breen, Daniels & Tomlinson, 2015; Timæus, Simelane & Letsoalo, 2013) such as access to sanitation or electricity (Mukeredzi & Mandrona, 2013). Some rural schools need basic infrastructure development (Gumbo, Jere & Terzoli, 2012) and are located in buildings constructed with mud (Skelton, 2014). Township and rural schools are often associated with low-quality education (Mestry, 2014) and ineffective management (Shepherd, 2016). These schools are also linked by the digital divide (Unicef, 2012), which refers to communities with limited or no access to the Internet or ICT infrastructure (Qureshi, 2012).

The digital divide is complex and extends to issues such as data availability and the access to or sharing of devices (Dalvit, Kromberg & Miya, 2014). Various stakeholders are investing in ICT for development (ICT4D) projects to bridge the digital divide in South Africa (Lewis, 2013; Unicef, 2012). Projects include providing access to ICT facilities at government facilities such as libraries and community centres (Dalvit, Kromberg & Miya, 2014; Lesame & Seti, 2014). ICT4D Living Lab computer laboratories (Gumbo, Jere & Terzoli, 2012) and cost-effective mobile applications (Dalvit, Kromberg & Miya, 2014) are also created.

Incorporating technology in schools is seen as one of the top priorities of bridging the digital divide (Gudmundsdottir, 2011). Teachers are expected to integrate new teaching and learning strategies, including technology, into their classrooms (Adegbenro & Gumbo, 2014; Adesote & Fatoki, 2013). The Internet is beneficial for education in so far as it can assist learners in obtaining information through search engines (Abbasi & Manawar, 2011; Olohunfunmi & Fajri, 2014), which assists in learning and overall school performance (Ktoridou, Eteokleous & Zahariadou, 2012). Access to the Internet also creates an opportunity for the development of e-learning and mobile learning platforms (Botha, Herselman & van Greunen, 2010) or support sites for learners and schools (Platz, Krieger, Niehaus & Winter, 2016). Mobile learning ICT enables a free-flow of information and communication between users (Gamreklidze, 2014). Learners use the Internet for social interaction with friends (Al-Khateeb & Epiphaniou, 2016; Amichai-Hamburger & Vinitzky, 2010), to play games and to search for information (Al-Jerbie & Jali, 2014). Through the use of social networking sites, the cyber world creates opportunities for children to socialise and reinforce feelings of acceptance from peers (Ktoridou, Eteokleous & Zahariadou, 2012).

The Internet provides opportunities, but also pose several risks for children (Teimouri, Hassan, Bolong, Daud, Yussuf & Adzharuddin, 2014). Dangers include creating and sharing inappropriate content, such as sexually explicit images (Aiken et al., 2015); (Jones, Mitchell & Walsh, 2012), exposure to online pornography (Nevondwe & Odeku, 2014) and cyber bullying (Popovac & Leoschut, 2012; Smit, 2015). Children need cyber-safety training (Manuputty, Noor & Sumardi, 2013; Tuukkanen & Wilska, 2015) and to address this need, Kortjan and Von Solms (2014) developed a five-layer cyber-security awareness and education framework which contains a sub-campaign for children.

1.4 Conceptual framework for cyber-security awareness and education campaigns in South Africa

The five-layer cyber-security awareness and education framework developed by Kortjan and Von Solms (2014) consists of a strategic, tactical, preparation, delivery, and monitoring layer. As indicated in Figure 1, the framework layers are supported by people, information, applications, infrastructure and financial capital (Kortjan, 2013).

The strategic layer considers the national vision, requirements, and expectations of cyber-security and the safety initiatives envisioned by the government (Kortjan & Von Solms, 2014), reflecting that governments are increasingly investing in cyber-security (Kshetri, 2013). Studies have called for national campaigns and participation by governments (Diga, Nwaiwu & Plantinga, 2013; Dlamini & Modise, 2012; Kritzinger, 2014) and therefore, the layer refers to the National Cyber-safety Policy, and the units tasked with the development of a strategic cyber-security plan (Kortjan & Von Solms, 2014).

The tactical layer follows the strategic layer. The South African National Cyber Security Policy Framework (NCPF) calls for the promotion of a cyber-safety culture, which is driven by the State through training, education, research, and skills-development programmes (Kortjan, 2013). The tactical layer proposes a national campaign called iWise Mzanzi; ‘i’ was selected to represent an informed and wise audience, which is cyber aware; while ‘Mzanzi’ refers to South Africa (Kortjan & Von Solms, 2014). The national campaign is supported by different private or public stakeholders (Kortjan & Von Solms, 2014). Kortjan (2013) proposed four sub-campaigns, or initiatives, consisting of a national awareness week; a community outreach programme; a campaign for all citizens; and a campaign aimed at schools. The preparation layer of the framework entails the topic, content and medium selection for these sub-campaigns (Kortjan & Von Solms, 2014). Once the content has been developed, the target audience for sub-campaigns or initiatives is identified and defined in the delivery layer (Kortjan & Von Solms, 2014).

The final layer is concerned with the control and evaluation of campaigns and initiatives to obtain feedback, identify the indicators of success and benchmark good practices (Kortjan & Von Solms, 2014). To plan successful campaigns, it is important to understand the communication process involved in the exchange of information (Gregory, 2010).

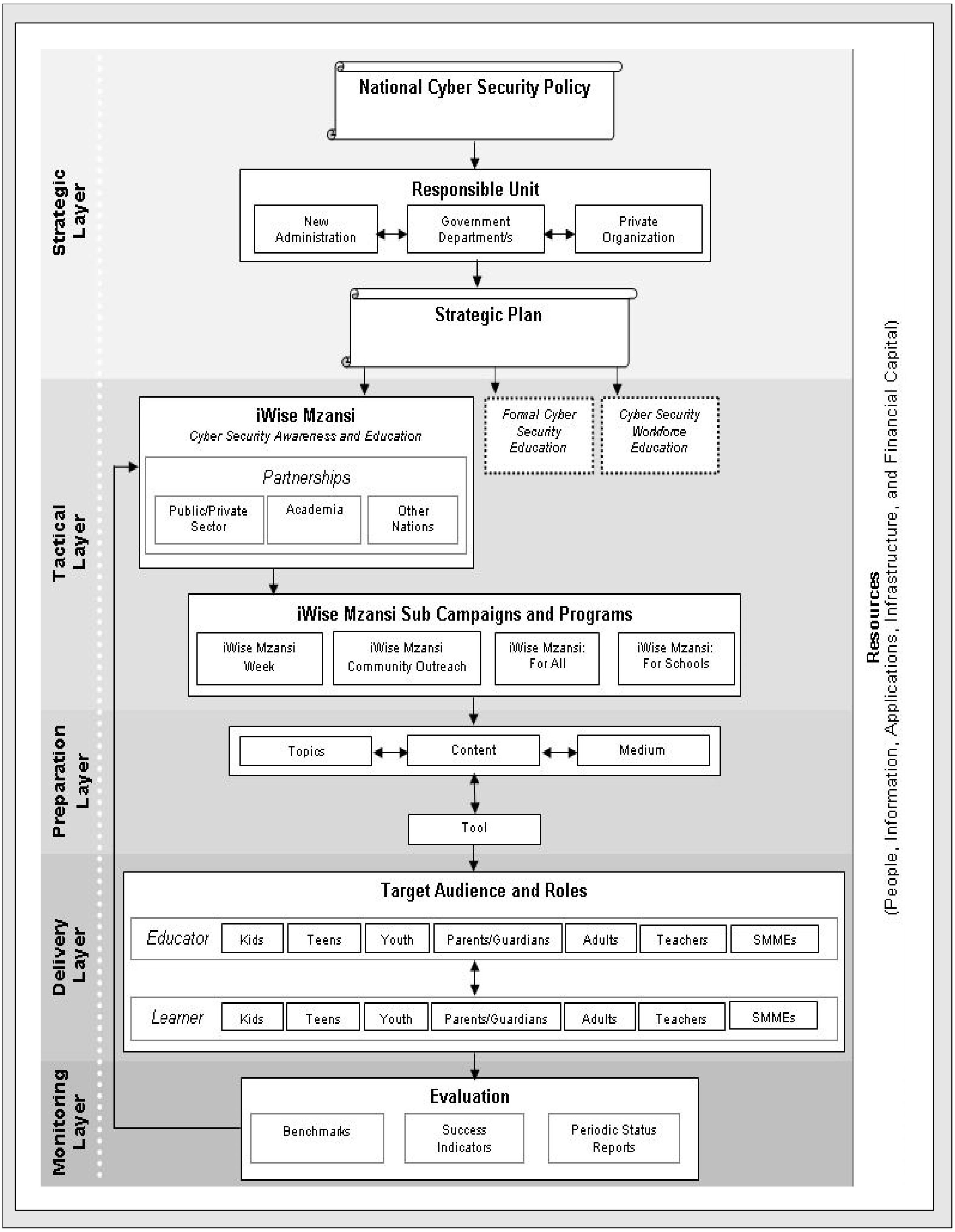


Figure 1. Conceptual framework for cyber-security awareness and education campaigns in South Africa (Kortjan, 2013)

1.5 Communication process

Before planning a campaign, the basic elements of the communication process should be understood by the campaign planner as it forms the foundation for the strategy used to communicate a message to a target audience. For this reason, two popular western representations of the stages involved in a communication exchange, the Shannon and Weaver linear model, and Osgood and Schramm circular model will be used to illustrate the communication process (Bandhiya & Joshi, 2015). Although the elements and focus of the two models differ, the process of communication is presented holistically when both models are studied. For this reason, the following section outlines the elements and process illustrated by the two models.

Figure 2 outlines the communication process which, according to the Shannon and Weaver model, includes an information source, sender, channel, receiver, destination, and noise (McKay, Marshall & Grainger, 2014).

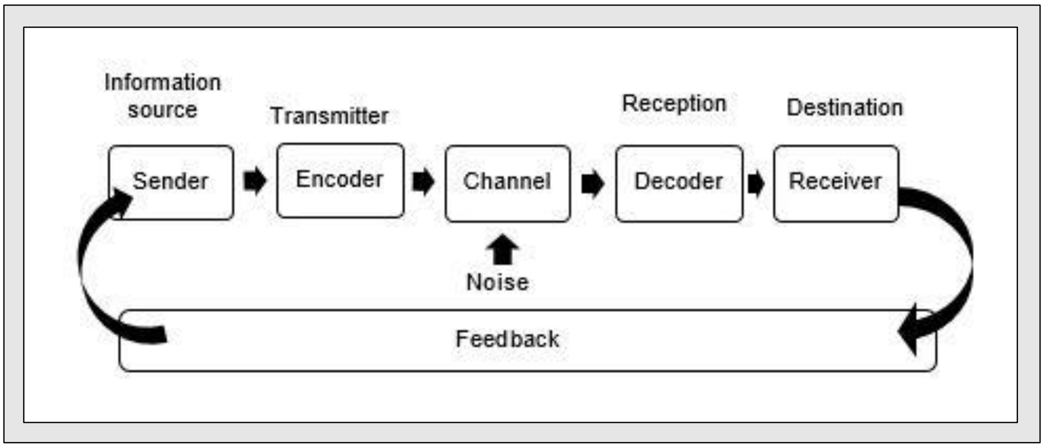


Figure 2. Shannon and Weaver model of communication
(Adapted from Al-Fedaghi (2012))

The sender of the information, seen as the information source, transmits a message through a channel to the receiver (Mazzei, 2014). The sender encodes the information by allocating meaning to the message, while the receiver decodes the information by interpreting the meaning of the message and provides feedback to the sender (Guttman, 2015). Along the way, the message can be distorted by noise which distracts from the message's meaning or intention (Laidre, Lamb, Schultz & Olsen, 2013). Distortion can be due to technical issues such as the effectiveness of symbols used (Adetunji & Sze, 2012), semantic issues such as whether symbols conveyed meaning (Grouchy, D'Eleuterio, Christiansen & Lipson, 2016), whether an exchange was successful

(Dimitrova, 2013); and whether the message had the intended effect (Epure, Eisenstat & Dinu, 2014). The Shannon and Weaver model highlights that the sender always has a specific end goal in mind when sending a message to the receiver (Harrison, 2014). In the case of a communication campaign, the purpose is to influence or change the behaviour of recipients by developing and sending messages through appropriate channels to reach the intended audience (Rice & Atkin 2013).

In contrast to the linear model of Shannon and Weaver which focuses on sending and receiving messages, the Osgood and Schramm Circular model focus more on the interpretation of messages through the process of encoding and decoding (Popescu, Pârgaru, Popescu & Mihai, 2015). Figure 3 illustrates the circular nature of the Osgood and Schramm circular model of communication. The sender and receiver both continuously encode and decode messages cognitively (Guttman, 2015; Turnitsa, 2013).

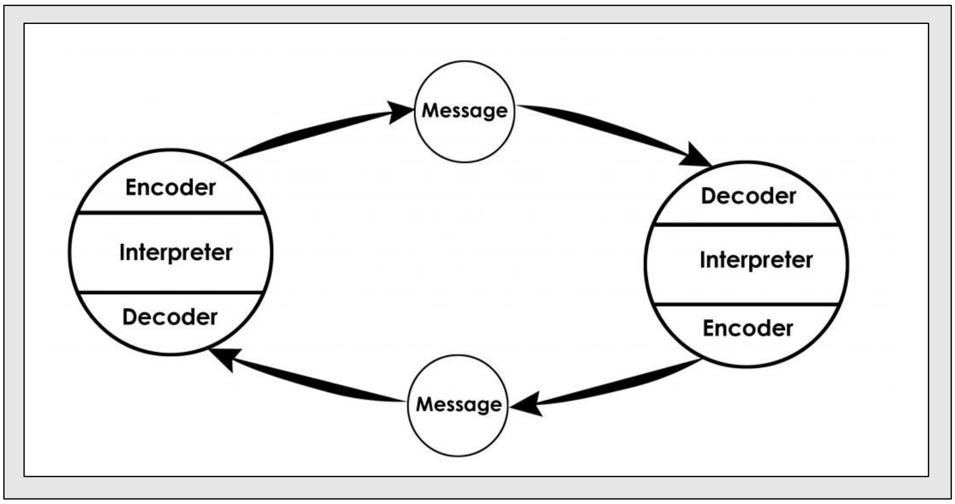


Figure 3. Osgood and Schramm circular model of communication (Adapted from Elkins, Derrick, Burgoon & Nunamaker (2011))

Senders and receivers use denotative and connotative interpretation to understand the messages communicated during the information exchange (Kropp, 2015). Denotative interpretation refers to analysing a message in a factual or simple way, whereas connotative interpretation considers meaning in context (Anand, 2014).

In summary, the Shannon and Weaver linear model, and Osgood and Schramm Circular model illustrate the elements contained in the process of communication. Although these models are not used as frameworks for campaign planning, the fundamentals of communication is an important consideration in campaign planning (Rice & Atkin, 2013). According to the Shannon and Weaver model, a message can be distorted by noise, which will influence whether a message will be received and interpreted as intended (McKay, Marshall & Grainger, 2014). Campaign planners, therefore, need to consider factors which contribute to distortion when designing the message and selecting the tools or mediums to deliver the message. The Osgood and Schramm Circular model show that messages can be interpreted in different ways, which can lead to message distortion when receivers interpret information differently to what was intended by the sender (Popescu, Pârgaru, Popescu & Mihai, 2015). Campaign planners, therefore, need to consider the denotative and connotative interpretation of the symbols used in their communication exchanges.

With a basic understanding of the communication process, a campaign planner can consider several theories which address elements of campaign development (Rice & Atkin, 2013). As no communication theory exists which encompasses all aspects of campaign planning (Rice & Atkin, 2013), an integrated approach will be used for the study, by combining elements from the fields of communication, public relations and social marketing (Smith, 2012; Šramová, 2015).

Six approaches used for campaign planning will be discussed in chapter four of the dissertation. The first approach refers to the campaign principles proposed by Wilcox and Cameron (2014). The principles contain seven stages and were developed for public relations campaigns. The second program and campaign planning framework, developed by Cornelissen (2014), consists of six stages and was developed for communication campaigns. The third approach, suggested by Perloff (2014), is used for social marketing campaign planning and has five stages. Social marketing applies promotion principles to campaigns encouraging some form of social change in society (Kubacki, Rundle-Thiele, Lahtinen & Parkinson, 2015; Lefebvre, 2013). The fourth approach refers to The Public Relations Institute of Southern Africa's (PRISA) seven steps for programme planning (Skinner, Mersham & Benecke, 2013). The fifth approach contains the planning stages for public relations campaigns summarised by Gregory (2010). The sixth approach considers the steps required for the development of effective communication campaigns proposed by Kotler, Armstrong and Tait (2010). Campaigns need to be managed and executed in a logical sequence, which is proposed by the framework developed by Kortjan and Von Solms (2014).

1.6 Rationale

Kortjan and Von Solms (2014) addressed the need for a South African framework for cyber-safety awareness. Kortjan (213) supports the strategic and tactical layers of the proposed framework with several examples from global studies and initiatives to indicate how it was developed, but the preparation, delivery and monitoring layers of the framework can be developed further. The purpose of this study will be to refine the preparation and delivery layers, while the refinement of the monitoring layer can be addressed by future studies through the integration of communication, business management and IT theory.

The preparation and delivery layers can be developed through the integration of communication theory. According to Kortjan (2013), the target audience would influence the topic and content selection during the preparation layer. The audience, however, is only defined by the next layer, called the delivery layer, which follows the preparation layer. The topic, content, medium and tools are interrelated and selected for an audience who is defined only by the delivery layer. Not identifying a target audience at the outset to determine how cyber-safety best practices are learnt can lead to campaign failure (Korpela, 2015).

It is important to target specific audiences when planning campaigns (Ridley, 2015). According to communication research, the target audience should be identified and described before developing campaign material (Mayasari, 2012; Nathanail & Adamos, 2013; Thaler & Helmig, 2013). Identifying the target audience ensures that the characteristics of the messages and the channels used appeal to the message recipients (Andreu, Casado-Díaz & Mattila, 2015; Ferguson & Phau, 2013; Yoon & Tinkham, 2013).

Campaigns need to achieve maximum impact (Babooram et al., 2010). Not only has running campaigns become increasingly expensive (Evans-Lacko, London, Little, Henderson & Thornicroft, 2010), but it is also difficult to reach the intended audience in a cluttered media environment (Taylor, 2013; Urwin & Venter, 2014). Consequently, it is essential to plan and execute cyber-safety and awareness campaigns efficiently (Aloul, 2012; Kajzer et al., 2014).

As indicated in Figure 4, there is an overlap between IT and communication theory when planning cyber-safety campaigns. By incorporating the two fields, the interdisciplinary study can contribute towards developing effective cyber-safety campaigns. This observation leads to the rationale for the study.

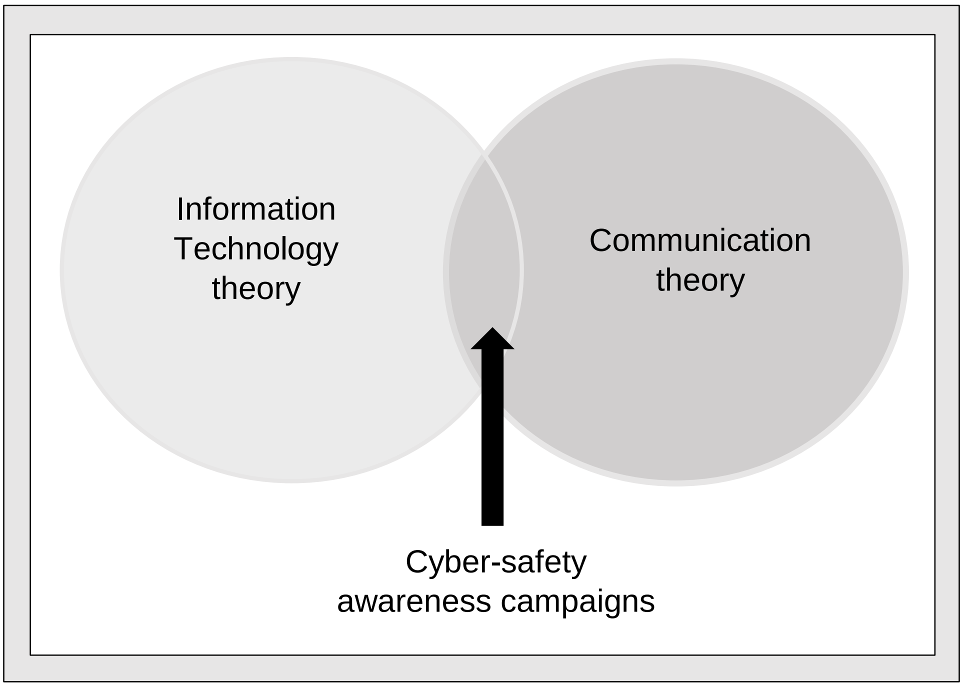

Information Technology theory
Communication theory
Cyber-safety awareness campaigns

Figure 4. Overlap between cyber-safety and communication

By incorporating theory from the two fields, the interdisciplinary study builds on and adds to the growing literature on the development of cyber-safety awareness and educational initiatives.

1.7 Purpose of the study

The purpose of the research is to refine the preparation and delivery layers of the proposed cyber-safety awareness and educational framework for South Africa, as developed by Kortjan and Von Solms (2014), through the integration of communication theory in the framework.

To refine the scope of the research and to ensure that the study provides a clear contribution to the field, the focus is on children as they form the target audience for iWise-Mzanzi:For Schools, which is a sub-campaign of the framework.

1.8 Research question

The following research question must be addressed to fulfil the purpose of the study: What are the elements required for the preparation and delivery of a cyber-safety awareness campaign aimed at children?

1.9 Research objectives

The following research objectives guide the study:

I. To identify, using the existing literature, the essential elements required for conducting a cyber-safety awareness campaign for children;

II. To describe an existing South African cyber-safety awareness campaign aimed at schools, which forms the single case study;

III. To compare the case study with the identified elements, and to determine whether there are any application gaps and areas for improvement;

IV. To make recommendations for improved and integrated strategies for cyber-awareness campaigns aimed at school children in South Africa.

1.10 Research design

A qualitative case study design was selected to fulfil the objectives of the study. According to Grbich (2013), qualitative research designs acknowledge the subjectivity of the researcher, consider what is truthful within the context and at the time when the research conducted and takes on a holistic approach.

A summary of the research methodology used for the study is provided in Table 1, followed by a brief discussion of how the research design will assist in meeting each research objective.

Table 1. Overview of research design used for the study.

Research objective		Research design
I.	To identify, using the existing literature, the essential elements required for conducting a cyber-safety awareness campaign for children;	Literature review
II.	To describe an existing South African cyber-safety awareness campaign aimed at schools, which forms the single case study;	Case study
III.	To compare the case study with the identified elements, and to determine whether there are any application gaps and areas for improvement;	Data-driven thematic analysis
IV.	To make recommendations for improved and integrated strategies for cyber-awareness campaigns aimed at children in South Africa.	Based on analysis and findings from objective I and II

The following section briefly outlines the research design used to fulfil each objective:

1.10.1 Research Objective I

The first objective is to identify, using existing literature, the essential elements required for conducting a cyber-safety awareness campaign in South Africa.

The first objective is addressed through a literature review. From an IT perspective, there is a need for cyber-safety awareness, and educational initiatives to influence user behaviour (Grobler, Jansen van Vuuren & Zaaiman, 2011; Kritzinger & von Solms, 2012; Walaza, Loock & Kritzinger, 2014). Chapter three of the dissertation provides literature on the essential elements required to conduct a cyber-safety awareness campaign for children. From a communication perspective, six campaign planning models are reviewed and integrated into cyber awareness campaign planning. Chapter four of the dissertation provides literature on the requirements for campaign planning from a communication perspective.

1.10.2 Research Objective II

The second objective is to describe an existing South African cyber-safety awareness campaign aimed at schools, which forms the single case study.

A qualitative case study design guides the research. Case studies can be used to describe, explain or predict various phenomena (Boblin, Ireland, Kirkpatrick & Robertson, 2013; Woodside, 2010). According to Simons (2015), case study research can also be used to test or build on existing theory. A case study refers to a bounded system which requires a clear description of what the case refers to and what it includes or excludes (Creswell, 2013; Rule & John, 2015). Researchers can focus on a single case or multiple cases (Dasgupta, 2015; De Massis & Kotlar, 2014). If a single case is selected, in-depth information and knowledge are obtained, as content accessed and gathered is relevant to a specific example or situation (Rule & John, 2015; Thomas, 2011).

For the purpose of the study, the South African Cyber Security Academic Alliance (SACSAA) cyber-safety campaign forms the bounded system for this study. Researchers from the University of Johannesburg (UJ), the University of South Africa (UNISA), and Nelson Mandela Metropolitan University (NMMU) formed SACSAA in 2011 to equip South African citizens with the cyber-security knowledge and the skills required to protect themselves from dangers online (Kortjan & Von Solms, 2014).

In response to the need for cyber-safety awareness and training for children, SACSAA developed a two-part educational campaign aimed at children, educators and parents (SACSAA, 2016). According to the SACSAA website (cyberaware.org.za), the first part of the campaign consists of educating children about cyber-safety risks. The second part of the campaign allows children to apply their knowledge through a poster contest

According to Yin (2013), qualitative research studies frequently use purposive sampling, which is described as selecting a sample that is most pertinent to a study (Creswell, 2013; Flyvbjerg, 2006; Ridley, 2015). The SACSAA campaign material serves as the sample for the study and includes the SACSAA website (www.cyberaware.za) and all campaign documentation available on the SACSAA website. A letter from SACSAA, granting permission for the use of the material as part of the study, is attached as Appendix A.

1.10.3 Research Objective III

The third objective is to compare the case study with the identified elements and to determine whether there are any application gaps and areas for improvement.

The essential elements for campaign planning identified from Information Technology and Communication Science literature, are compared to the SACSAA campaign in chapter five. A data-driven thematic analysis is used to identify and compare the elements (Malterud, 2012) identified as essential for the planning and delivery of a campaign, with the SACSAA campaign. The analysis process includes skimming, reading, analysing and interpreting the data (Bowen, 2009; Creswell, 2013; Schreier, 2012) to identify patterns, which leads to the development of themes (Bowen, 2009; Frededay & Muir-Cochrane, 2006). The themes are presented in the form of a SWOT analysis, which refers to a summary of the strengths, weaknesses, opportunities and threats associated with the SACSAA campaign (Monzani, Ripoll, Peiró & Van Dick, 2014).

1.10.4 Research Objective IV

The fourth objective is to make recommendations for improved and integrated strategies for cyber awareness campaigns in South Africa. Recommendations are outlined in chapter six. Recommendations are made for the proposed refined preparation and delivery layers of the cyber-security awareness, and education framework, based on the current strengths and weaknesses, as well as future opportunities and threats associated with the SACSAA campaign.

1.11 Implementation of validity and reliability principles

Reliability, or trustworthiness, is important throughout the study; and is especially applicable to the collection, and analysis phase of data and reporting of findings (Maree, 2007). Humans are subject to biases and therefore it is important to consider the reliability of findings (Woodside, 2010). Different sources of verified data and a detailed record of the research process contributes to the reliability of findings (Maree, 2007). The research takes an interdisciplinary approach, and several sources of information (Yin, 2013) and theoretical perspectives are used to obtain information to validate the discussions contained in the study (Creswell, 2013). To further contribute to the trustworthiness of the study, data analysis is clearly explained by relevant literature and supported by visual elements, such as illustrations (Riege, 2003).

Communication studies use argumentation when determining the persuasiveness of messages (Xu & Zhang, 2012); scientists use argumentation to justify the use and application of theoretical frameworks or models in studies (De Sá Ibraim & Justi, 2016); and the legal profession uses argumentation as logical reasoning to defend or attack a point of view (Prakken & Sartor, 2015). For the present study, interpretation of evidence (Kane, 2013; Prakken & Sartor, 2015), based on the review of literature and application of the case study, will be used as an argument for the proposed refinements of the framework.

1.12 Assumptions, limitations, and scope

There are four forms of delimitation applicable to case studies, as outlined by Rule and John (2015), namely:

- Category delimitation, which refers to the case study, in this instance focusing exclusively on the SACSAA cyber-safety campaign, and the focus on two of the five framework layers;
- Spatial delimitation, which in this study applies to the South African context;
- Temporal delimitation, as the case study represents the work of one academic alliance between 2011 and 2016; and

- Thematic delimitation, as the case study only includes content applicable to the cyber-safety awareness and educational framework developed for South Africa.

1.13 Significance of the study

By adopting a communication perspective on cyber-safety research, this interdisciplinary study can assist cyber-safety researchers to refine and, in future, to implement a more effective cyber-safety awareness and educational framework. The implementation of an improved framework contributes to the creation of a cyber aware and cyber-safe culture in South Africa as described by Von Solms and Von Solms (2014).

1.14 Dissertation structure

The dissertation is outlined according to the writing structure proposed by Creswell (2013) and consists of an entry vignette, introduction, description of the case and context, an overview of the development of issues, a summary of assertions or lessons learnt and a closing vignette. A table outlining the structure and research objectives addressed by the study introduces each chapter.

1.15 Definition of terms

The following terminology is defined in the context of the research:

Communication campaign: refers to a short-term planned attempt to inform, educate and persuade a target audience (Guttman, 2015).

Communication programme: relates to the long-term integration of various communication campaigns and activities to contribute to the strategic management of a project or organisation (Mohamad, Abu, Halim, Rageh, Bakar, Halim & Ismail, 2014).

Cyber awareness: having knowledge about cyber risks associated with the online world and using the knowledge to be alert to possible online dangers.

Cyber awareness training: relates to all initiatives developed and implemented to educate users about the risks associated with the online world (Saridakis et al., 2016).

Cyber-ethics: relates to acting within the moral and ethical guidelines expected by society when working online (Pusey & Sadera, 2011).

Cyber-safety: refers to behaviour and best practices linked to acting responsibly in the digital world (Pusey & Sadera, 2011).

Cyber-security: refers to computer systems implemented to protect computer hardware and software from malware (Pusey & Sadera, 2011).

Digital citizen/ Digital citizenship: relates to the online identities and behaviour of users in the online world (Isman & Gungoren, 2013).

Stakeholder(s): are internal and external audiences who influence or are influenced by an organisation or project (Fassin, 2011).

1.16 Conclusion

Chapter one confirmed the importance of cyber awareness education. Different terminology has been used to describe the process of cyber awareness, but the key is ensuring that users are equipped with the skills required to be safe online. At risk users such as children can be reached through communication campaigns, but these initiatives need to be structured and coordinated in a coherent manner.

South African children are faced with many challenges caused by socio-economic factors, problems with the management of school systems, and national problems such as the amount of violence experienced in the country. These challenges lead to circumstances which make South African children vulnerable to online exploitation.

To ensure that children are aware of online dangers, Kortjan and Von Solms (2014) developed a conceptual framework for cyber-security awareness and education campaigns in South Africa. Although the framework was developed for a cyber-security context, the integration of communication theory can assist in refining the preparation and delivery layers of the framework, to ensure that it can be implemented in future. The interdisciplinary study, therefore, aims to contribute to the creation of a cyber-safe culture in South Africa by refining the preparation and delivery layer of the cyber-safety awareness and educational framework, through the integration of communication theory. To fulfil the purpose of the study and to make a clear contribution to cyber-security awareness efforts, the focus is placed on campaigns for children as they form the target audience for iWise-Mzanzi: For Schools, which is a sub-campaign of the framework. The research design used to fulfil the purpose of the study is discussed in the following section.

CHAPTER 2 RESEARCH METHODOLOGY

“Would you tell me, please, which way I ought to go from here?"
"That depends a good deal on where you want to get to."

(Lewis Carroll, Alice's Adventures in Wonderland)

<table>
<tr><td colspan="3"><b>Entry vignette</b>
Abstract</td></tr>
<tr><td colspan="3"><b>Introduction to case and context</b>
Chapter one: Introduction
<b>Research question:</b>
What are the elements required for the preparation and delivery of a cyber-safety awareness campaign?</td></tr>
<tr><td colspan="3">Chapter two: Research methodology</td></tr>
<tr><td rowspan="3"><b>Research objective I.</b>
To identify, using existing literature, the essential elements required for conducting a cyber-safety awareness campaign in South Africa.</td><td colspan="2"><b>Description of case and context</b></td></tr>
<tr><td>Chapter three: Cyber-safety in South Africa</td><td>Chapter four: Campaign planning</td></tr>
<tr><td><i>Information Technology perspective</i></td><td><i>Communication Science perspective</i></td></tr>
<tr><td><b>Research objective II.</b>
To describe an existing South African cyber-safety awareness campaign aimed at schools, which forms the single case study;</td><td colspan="2" rowspan="2"><b>Development and detail about selected of issues</b>
Chapter five:
SACSAA campaign</td></tr>
<tr><td><b>Research objective III.</b>
To compare the case study with the identified elements, and to determine whether there are any application gaps and areas for improvement;</td></tr>
<tr><td><b>Research objective IV.</b>
To make recommendations for improved and integrated strategies for cyber awareness campaigns in South Africa.</td><td colspan="2"><b>Lessons learnt and closing vignette</b>
Chapter six:
Conclusion
Findings and recommendations</td></tr>
</table>

2.1 Introduction

A detailed record of the research process contributes to the reliability of findings (Maree, 2007), and therefore, chapter two provides an overview of the qualitative research methodology which guides the study.

The structure of a study depends on the research design selected (Yin, 2013). Rule and John (2015), state that there are no research approaches which should be seen as more significant when compared to others, as the method chosen by the researcher links directly to the purpose, research question, objectives and the type of study undertaken.

The purpose of the study is to refine the preparation and delivery layers of the proposed cyber-safety awareness and educational framework for South Africa, as developed by Kortjan and Von Solms (2014), through the integration of communication theory. To refine the scope of the research, and to ensure that the study provides a clear contribution to the field, the focus is on children as they form the target audience for iWise-Mzanzi:For Schools, which is a sub-campaign of the existing framework.

To fulfil the purpose of the study, four objectives have to be met. The first objective of the study is to identify, using the existing literature, the essential elements required for conducting a cyber-safety awareness campaign for children. A review of relevant Information Technology and Communication Science literature leads to the identification of key components of campaign planning. The second objective of the study is to describe an existing South African cyber-safety awareness campaign aimed at schools, which forms the single case study. Chapter two provides an overview of the qualitative case study design, and explains the procedure followed to analyse the SACSAA campaign, which serves as the case study. The analysis of the SACSAA campaign data, links to the third objective, which is to compare the case study with the elements required for campaign planning, and to determine whether there are any application gaps and areas for improvement. The analysis results are used to meet the fourth objective, which is to make recommendations for improved and integrated strategies for cyber-awareness campaigns aimed at school children in South Africa.

Following the explanation of the procedure followed for analysing the case study, the chapter concludes with an overview of the ethical considerations relevant to the study.

2.2 Research design

A qualitative approach is adopted for the study, because qualitative research is characterised by the need to gain a deeper understanding of phenomena (Sommerfeldt, Kent & Taylor, 2012) through exploring rich descriptive content about relevant subject matter (Tracy, 2013).

According to Creswell (2013) qualitative studies take the form of narrative research, phenomenology, grounded theory, ethnography, or case studies. Narrative research is associated with exploring and presenting experiences of individuals through story-telling (Lewis, 2015). Phenomenology constructs meaning from individual experiences or texts and finds commonalties shared by a phenomenon (Creswell, 2013; Grbich, 2013). Grounded theory draws on experiences and observations of social exchanges, procedures or activities to produce theory (Creswell, 2013). Ethnography studies requires researchers to join and observe groups who share the same characteristics to analyse the behaviour of the group culture (Creswell, 2013). Case studies are used to describe, explain or predict everyday phenomena through an in-depth investigation of a case (Boblin et al., 2013; Woodside, 2010).

Based on a review of the different approaches to qualitative research, a case study design is deemed most suitable to fulfil the purpose of the research. Classification of the purpose, approach and process applicable to case studies varies according to the author's perspectives (Thomas, 2011). According to De Massis and Kotlar, (2014) case studies can be classified as exploratory (when the purpose is to find out how something takes place), explanatory (when the purpose is to find out why something happens), and descriptive (to explain the relevance of something). Rule and John (2015) distinguish between case studies investigating issues with a broad scope (instrumental), and problems unique in nature (intrinsic). Creswell (2013) refers to intrinsic, instrumental and collective case studies. Instrumental case studies focus on a specific issue of concern, illustrated through a bounded system; intrinsic case studies concentrate on a given case; and collective case studies focus on several cases, which deal with the same issue of concern (Creswell, 2013).

A case study is seen as a unit of analysis (De Massis & Kotlar, 2014) or bounded system which requires a clear description of what the case refers to and what it includes or excludes (Boblin et al., 2013; Creswell, 2013). Researchers can use a single case or multiple cases to focus on (Dasgupta, 2015; De Massis & Kotlar, 2014). If a single case is selected, in-depth information and knowledge can be obtained, based on a specific example or situation (Rule & John, 2015; Thomas, 2011).

According to (Simons, 2015), case study research can also be used to test or build on existing theory. The approach used for a case study analysis, depends on the purpose of the study (Yin, 2013). Figure 5 illustrates that existing theory, concepts and methodologies are verified through its application to a case. An existing theory can be developed further to suit a specific context or case (Rule & John, 2015).

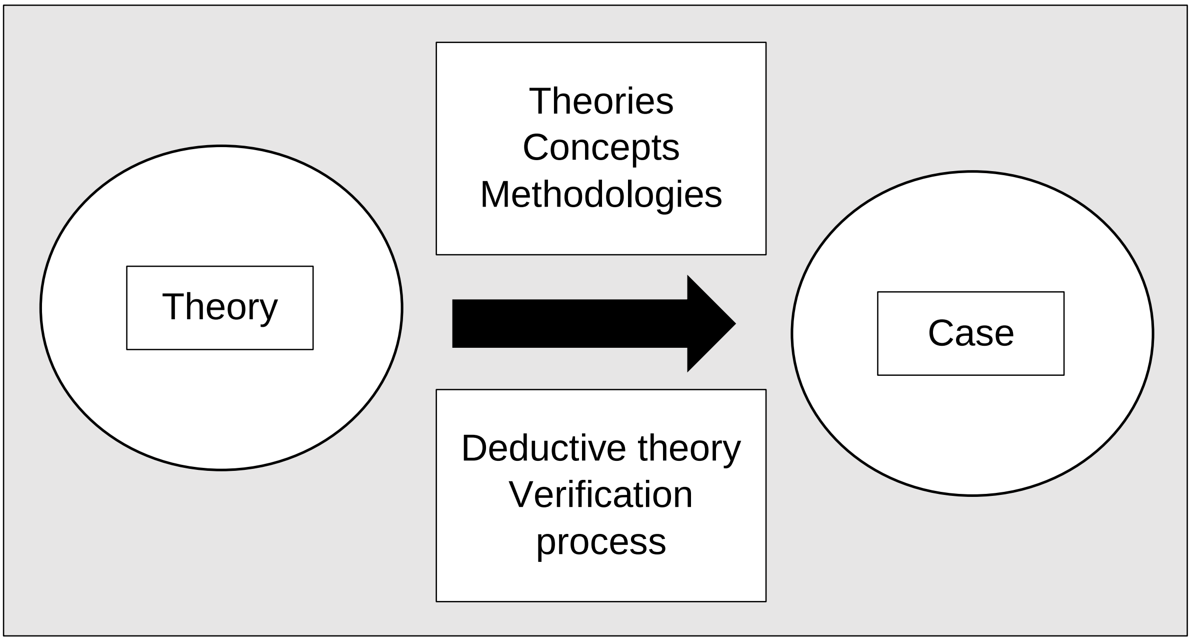


Figure 5. Theory-first approach to case (Rule & John, 2015)

A theory-first approach applies to this study, because existing communication theories and concepts will be used to analyse a South African cyber-safety awareness campaign (Rule & John, 2015; Yin, 2013).

2.3 Advantages of using case study approach

The advantages of case studies are in-depth knowledge, flexibility in the range and scope of research studies, the versatility and accommodating nature towards other research approaches, the manageability and flexibility in the range and scope of research studies as the key advantages of case studies (De Massis & Kotlar, 2014; Rule & John, 2015; Simons, 2015).

2.4 Challenges of using case study approach

The challenges of using case study approach often link to the validity and reliability of the research. Reliability refers to the trustworthiness of a study (Elo, Kääriäinen, Kanste, Polkki, Utriainen & Kyngas, 2014); and it is essential that the necessary safeguards are shown to have been put in place for the collection, analysis and reporting of the data to be considered valid (Maree, 2007). Not least, researchers are subject to their biases (Watkins, 2012), which makes it important to consider the trustworthiness of the findings (Kapoulas, 2012; Woodside, 2010). The trustworthiness of research based on a case study increases through triangulation by using different sources of data, providing detailed descriptions (Zimmerman, 2014); verifying data throughout the process, and keeping a detailed record of the research process (Houghton, Casey, Shaw & Murphy, 2013).

Scholars question the rigour of case study research (Gibbert & Ruigrok, 2010), and remark that single-case study research cannot contribute significantly to the development of knowledge, as findings from the research cannot be generalised (Gibbert & Ruigrok, 2010). This, together with the impact of researcher biases based on personal experiences or frame of references, and the difficulty in comparing research findings are aspects of the criticism of case study research (Rule & Vaughn, 2011; Thomas, 2011).

Maree (2007) explains that the purpose of case study research is not to generalise, but to provide insight into a specific case, context or concept (Yin, 2013). According to Riege (2003), the validity of case-study research focuses on construct validity, internal validity and external validity (Gibbert & Ruigrok, 2010). Construct validity considers the concepts studied within a specified context (Rowley, 2002), and increases by using several sources of information and through peer review of case documentation (Riege, 2003). Internal validity is increased by clearly explaining and supporting content, which may be achieved with visual elements such as illustrations (Riege, 2003). External validity increases by considering the domain or context, and whether the study is replicable in the identified domain (Rowley, 2002). External validity also increases by outlining the limitations of the research, supporting statements with relevant literature and discussing the findings within the context of the study (Riege, 2003).

Another challenge deemed applicable to the present study revolves around the debate concerning the importance of practical knowledge, seen as context-dependent knowledge, and theoretical knowledge, which is considered to be context-independent knowledge (Flyvbjerg, 2006). Case studies provide concrete context-dependent knowledge and knowledge gained through the research design (Simons, 2015). The different contexts of the research can be varied and may include culture, politics, and policies which are interlinked and contribute towards producing meaning for the framework of the study (Simons, 2015).

The validity of a study depends on the data collection process followed (Hashemnezhad, 2015). With this in mind, the procedure for conducting a case study proposed by Creswell (2013) was selected as it provides structure to the case study research process. The process followed is outlined according to the following steps: identifying the case, collecting data, identifying and analysing themes, and, finally, reporting the meaning of the case (Creswell, 2013).

2.5 Procedure followed for the study

The following section outlines the procedure used for the study:

2.5.1 Select existing theory

A theory-first approach is used for the study. Chapter three and chapter four of the dissertation explore the key elements required to carry out a successful cyber-safety awareness campaign for children. A review of the relevant cyber-safety and communication literature in these chapters, leads to the identification of themes from existing theory (Rule & John, 2015; Yin, 2013). Next, the themes are applied to a case study.

2.5.2 Identify case

A single case approach is used for the study because the focus of the research is on one continuous cyber-safety campaign, developed by SACSAA, which is founded upon an alliance of academic institutions. As the selected case, SACSAA is representative of the work of different academic institutions and serves as an example of a cyber-safety initiative in the South African context.

2.5.3 Collect data

Data relevant to the purpose of the study is collected. The SACSAA material constitutes the data for the case. Analysing documentation is valuable to case study research because it is an efficient method for collecting data which are available and is cost-effective, precise and unobtrusive (Bowen, 2009).

The sample includes the SACSAA website (www.cyberaware.za), and all campaign material available on the site, including pamphlets and a workbook developed for children and teachers. Permission was granted from SACSAA to use the campaign material as a sample (Appendix A).

2.5.4 Identify and analyse themes

During the next step, a thematic analysis is used to identify themes in the existing SACSAA campaign material (Creswell, 2013). Thematic analysis refers to the process of identifying connections between domains (Onwuegbuzie, Leech & Collins, 2012).

Data sampled from existing sources (Schreier, 2012) can be used and is analysed inductively or deductively (Hashemnezhad, 2015). When searching for emerging codes or themes in the data inductive reasoning is used, while deductive reasoning uses existing theories and tests to identify themes in the data (Hashemnezhad, 2015). Reviewing existing documentation is valuable to case study research as the data is available, cost-effective, and precise and collection is unobtrusive (Bowen, 2009). The method includes skimming, reading, analysing and interpreting the data (Bowen, 2009; Creswell, 2013; Schreier, 2012). When using data-driven thematic analysis, the researcher identifies any patterns during the data-analysis approach, which leads to the development of themes (Bowen, 2009; Frededay & Muir-Cochrane, 2006). According to Grbich (2013), the analysis includes the following stages: reading the database content; considering the data obtained and the research objectives; determining the data processing methods; making use of segmentation to identify areas requiring additional study and insight; grouping segments sharing characteristics; identifying any additional groups and label groupings; and applying the relevant theory and literature to the segmented groups.

The SACSAA material, which constitutes the data for the case, are analysed according to the key elements for carrying out a successful cyber-safety awareness campaign for children, identified in chapter three and chapter four. The SACSAA campaign is compared with the elements required for campaign planning, to determine whether there are any application gaps and areas for improvement. The qualitative thematic content analysis of SACSAA campaign material (Alhojailan & Ibrahim, 2012), leads to a summary of the strengths, weaknesses, opportunities and threats associated with the SACSAA campaign (Monzani et al., 2014).

2.5.5 Report meaning of case

The meaning of the case is reported in the form of recommendations for improved and integrated strategies for cyber-awareness campaigns aimed at children in South Africa. Argumentation based on theory (Chen & Wang, 2016) and evidence (Ibraim, Justi, De Sá Ibraim & Justi, 2016; Quigley, Burns & Stallard, 2015) from the SACSAA case study is used to justify the proposed changes to the framework.

2.6 Ethical considerations

The ethical standards of collecting and reporting on research data and findings, as outlined in the code of conduct for researchers at NMMU (Policy 404.01) are adhered to. Steps taken to ensure that the research remains ethical includes obtaining permission from SACSAA to use campaign material for the study, avoiding intentional bias, using information correctly, selecting an appropriate research design, and reporting findings accurately (Kumar, 2011).

The study does not include contact with any vulnerable groups and obtaining ethics clearance as prescribed by the NMMU policy on research ethics (Policy 404.02) are therefore not required.

2.7 Conclusion

Chapter two provided an overview of the qualitative research methodology implemented for the study. From the methods of inquiry recommended by Creswell (2013), a single case study design was deemed most appropriate for the purpose of the research. The purpose was confirmed as refining the preparation and delivery layers of the cyber-safety awareness and educational framework for South Africa (Kortjan & Von Solms, 2014), through the integration of communication theory. To refine the layers, a sub-campaign of the framework, called iWise-Mzanzi:For Schools (Kortjan & Von Solms, 2014), serves as an example of the process used for campaign planning.

A review of relevant IT literature in chapter three and Communication Science literature in chapter four leads to the identification of the main components of campaign planning. In chapter five, an existing South African cyber-safety awareness campaign aimed at schools is analysed and compared to the elements required for campaign planning as outlined in chapter three and four. The analysis highlights application gaps and areas for improvement which is presented in chapter six. The procedure outlined in chapter two guides the study and is implemented in an ethical manner to ensure that the contribution of the study is valid.

CHAPTER 3 CYBER-SAFETY EDUCATION

“Finding meaning, like losing meaning, involves pleasure as well as pain.”
(Lewis Carroll, Alice's Adventures in Wonderland)

<table>
<tr><td colspan="3">**Entry vignette**
Abstract</td></tr>
<tr><td colspan="3">**Introduction to case and context**
Chapter one: Introduction
Research question:
What are the elements required for the preparation and delivery of a cyber-safety awareness campaign?</td></tr>
<tr><td colspan="3">Chapter two: Research methodology</td></tr>
<tr><td rowspan="3">**Research objective I.**
To identify, using existing literature, the essential elements required for conducting a cyber-safety awareness campaign in South Africa.</td><td colspan="2">**Description of case and context**</td></tr>
<tr><td>Chapter three:
Cyber-safety in South Africa</td><td>Chapter four:
Campaign planning</td></tr>
<tr><td>*Information Technology perspective*</td><td>*Communication Science perspective*</td></tr>
<tr><td>**Research objective II.**
To describe an existing South African cyber-safety awareness campaign aimed at schools, which forms the single case study;</td><td rowspan="2" colspan="2">**Development and detail about selected of issues**
Chapter five:
SACSAA campaign</td></tr>
<tr><td>**Research objective III.**
To compare the case study with the identified elements, and to determine whether there are any application gaps and areas for improvement;</td></tr>
<tr><td>**Research objective IV.**
To make recommendations for improved and integrated strategies for cyber awareness campaigns in South Africa.</td><td colspan="2">**Lessons learnt and closing vignette**
Chapter six:
Conclusion
Findings and recommendations</td></tr>
</table>

3.1 Introduction

Connectivity is seen as a basic right by some users (Oyedemi, 2015), but everyone does not have access to the Internet (Ponelis & Holmner, 2015). The use of technology for communication, recreation, collaboration and economic purposes on the African content is, however, increasing (Futcher, Schroder & von Solms, 2010; Kritzinger & von Solms, 2012; Shillair, Cotten, Tsai, Alhabash, LaRose & Rifon, 2015). As a developing continent, countries can be subject to cyber insecurity (Jansen Van Vuuren, Phahlamohlaka & Brazzoli, 2010) and may not have access to the resources required to fight cyber-attacks (Gamreklidze, 2014). Citizens may also be unaware of the risks associated with technology use (Grobler et al., 2011) due to a lack of awareness initiatives (Alavi, Islam & Mouratidis, 2016; Von Solms & Von Solms, 2014).

Even though the cyber world has an international span (Choucri, Madnick & Ferwerda, 2014; Ktoridou, Eteokleous & Zahariadou, 2012; Kayworth & Whitten, 2010) governments can be held accountable for cybercrimes, such as cyber-attacks, committed by their citizens (Ridley, 2015). Cyber-security is therefore both a national and a global priority which warrants international cooperation (Bendovschi, 2015; Menon & Siew, 2012). South Africa signed the International Treaty on Cybercrime (Kshetri, 2015) and, in 2012, introduced The National Cyber-safety Policy Framework (NCPF), which is driven by the State through training, education, research, and skills-development programmes (Sonhera, Kritzinger & Loock, 2015). The implementation of cyber-safety legislation (Stewart & Lacey, 2012) should have the end goal of creating a societal-wide cyber-safety culture (Choucri, Madnick & Ferwerda, 2014; Gcaza, Von Solms & Van Vuuren, 2015; Reid & Van Niekerk, 2014), and therefore requires support from various stakeholders to integrate awareness initiatives (Grobler et al., 2011).

Kortjan and Von Solms (2014) proposed a cyber-safety education framework for South Africa to coordinate awareness campaigns. Chapter three describes the layers of the framework and integrates theory relating to the development of campaigns for children. The strategic, tactical and delivery layers of the framework are discussed briefly as it relates to the preparation and delivery layer, which is the focus of the study. The preparation layer and delivery layer is discussed more extensively to review the selection of topics, content, mediums and tools as well as define the intended audience.

The chapter concludes with a summary of the key elements discussed and introduces the next literature review chapter which covers campaign planning from a Communication Science perspective.

3.2 Cyber-safety education framework

Kortjan and Von Solms (2014) proposed a cyber-safety education framework for South Africa which consists of a strategic, tactical, preparation, delivery and monitoring layers. The implementation phase of such initiatives is challenging and often depends on the resources available (Gamreklidze, 2014; Muller, 2015; Swart, Irwin & Grobler, 2014). The framework, therefore, considers people, information, applications, infrastructure and financial capital as resources required to implement the framework (Kortjan & Von Solms, 2014). Although the focus of the study is in the preparation and delivery layer of the framework, a brief overview of the resources, and the strategic, tactical and evaluation layers is deemed necessary as it informs the development of the preparation and delivery layer.

3.3 Strategic layer

A strategic approach to cyber-safety is required to gather intelligence on current or further developments (Buono, 2014). As indicated in Figure 6, the responsible units for the execution of the National Cyber-security Policy, are government departments and private organisations supported by an administrative department.

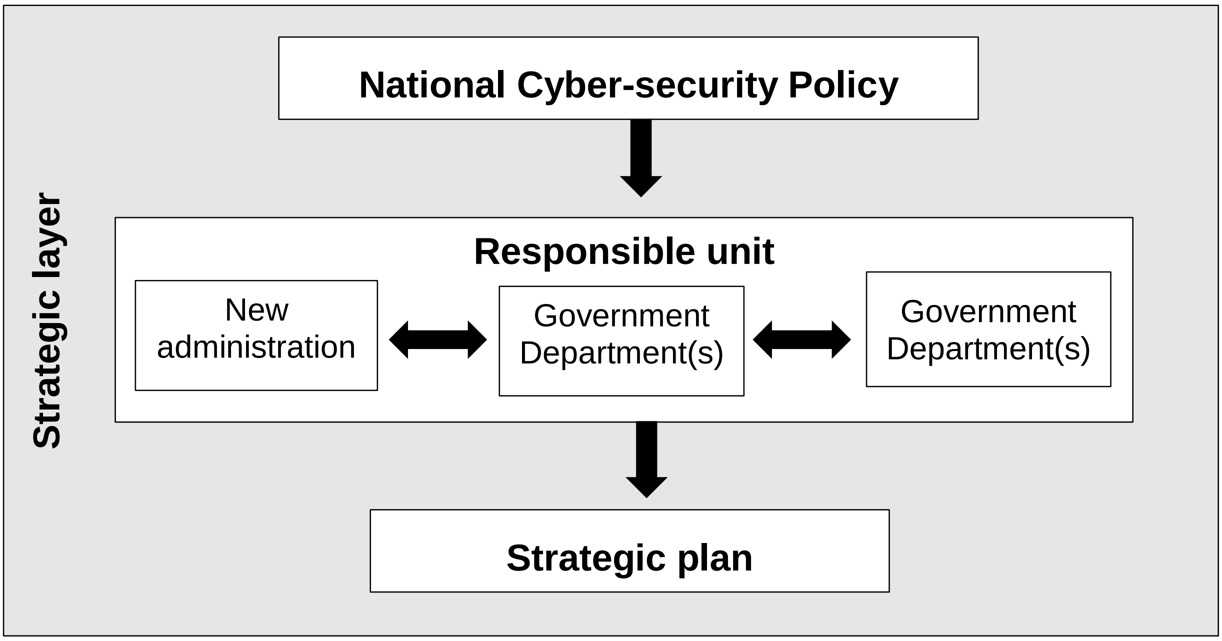


Figure 6. Strategic layer

Leadership from the government is required to implement cyber-safety legislation and awareness programmes (Buono, 2014; Davis, 2012). Governmental departments (Hope, 2015) and private organisations (Singh & Rishi, 2015) should, therefore, be supported by an administrative entity to drive and implement the National Cyber-safety Policy in South Africa (Kortjan & Von Solms, 2014). Several independent stakeholders have developed cyber awareness initiatives in South Africa (Dlamini & Modise, 2012), but, the initiatives from different stakeholders can be integrated into a strategic plan, which is then developed further in the tactical layer of the framework (Kortjan & Von Solms, 2014).

3.4 Tactical layer

Creating a cyber-safe culture (Gcaza, Von Solms & Van Vuuren, 2015) requires all Internet users to educate themselves about the risks associated with cyber use and implement a basic level of security (Tikk, 2011). Kortjan & Von Solms (2014) proposed a national campaign consisting of an annual national awareness week, community outreach, school campaign, and the creation of a cyber-safety resource website containing information for different stakeholders. According to Kritzinger and Von Solms (2012) a comprehensive national awareness campaign should be ongoing. As indicated by Figure 7, partnerships are required to sustain an ongoing campaign.

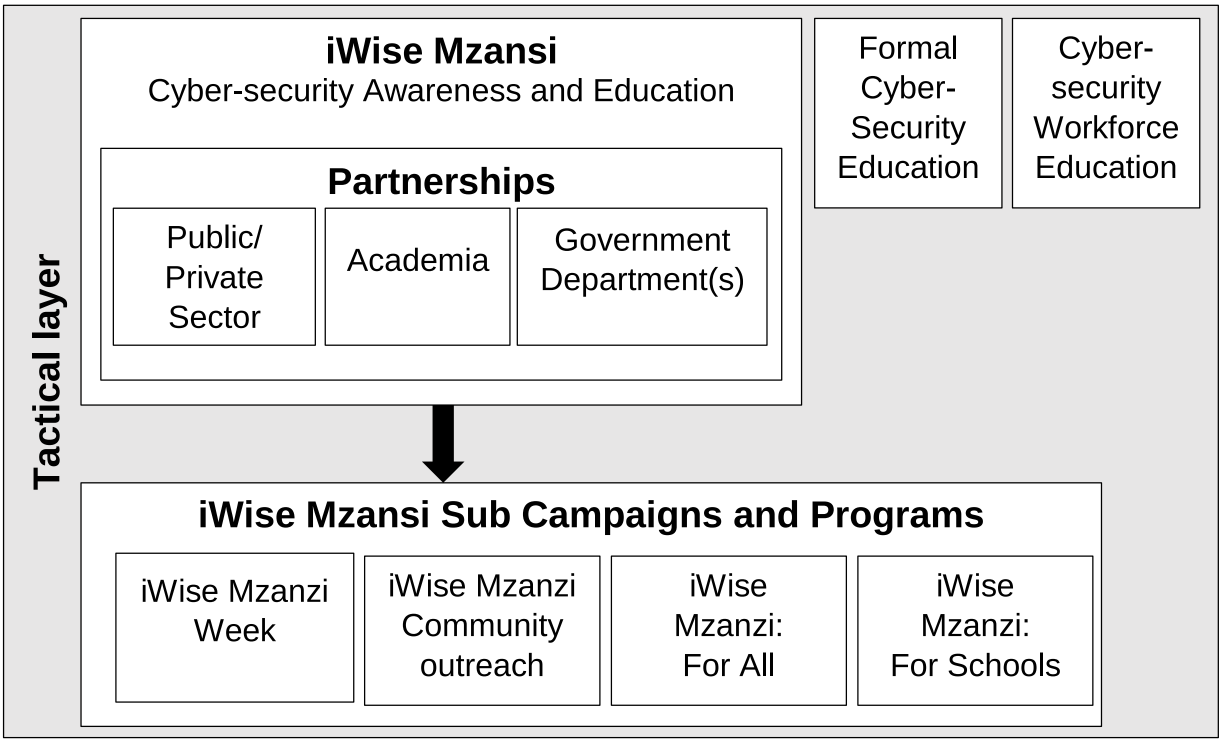

Tactical layer
iWise Mzansi
Cyber-security Awareness and Education
Partnerships
Public/ Private Sector
Academia
Government Department(s)
Formal Cyber-Security Education
Cyber-security Workforce Education
iWise Mzansi Sub Campaigns and Programs
iWise Mzanzi Week
iWise Mzanzi Community outreach
iWise Mzanzi: For All
iWise Mzanzi: For Schools

Figure 7. Tactical layer

Cyber-safety impacts the economy, and stakeholders from the businesses and private sector, as well as individual users, can be affected by online risks (Fourie, Sarrafzadeh, Pang, Kingston & Watters, 2014; Skopik, Settanni & Fiedler, 2016). It follows, therefore, that partnerships with stakeholders from the public and private sector are beneficial for cyber-safety initiatives (Salamzada, Shukur & Bakar, 2015; Ekos Research Associates, 2011).

Partnerships can include businesses who already allocate resources to the development of employee cyber awareness programmes (Blythe, 2013), and are required by the government to protect data of customers (Kayworth & Whitten, 2010). Non-profit organisations, such as Savvy Cyberkids, serves as an example of the collaboration with partners from industry and government departments to form global campaigns such as the STOP. THINK. CONNECT campaign (Kortjan, 2013). Academics can also contribute by conducting research in cyber-safety (Kortjan & Von Solms, 2014) and addressing the shortage of cyber-safety professionals (Fourie et al., 2014) to ensure that the number of professionals increases and have the latest skills. Academics can also facilitate workshops or seminars, and present cyber-safety public lectures to the community (Ktoridou, Eteokleous & Zahariadou, 2012).

3.5 Preparation layer

According to (Hansche, 2001), developing a cyber-safety awareness program involves the following steps: setting the goal/objectives, deciding on the level and type of content, choosing implementation and delivery options, overcoming obstacles such as financial or management support, and evaluating the effectiveness of the initiatives. Cyber awareness campaigns should have clearly defined objectives, an outline of the anticipated results, an overview of message delivery methods, a risk analysis, and evaluation plan (Dlamini & Modise, 2012). Kortjan and Von Solms (2014) incorporated these steps and refer to the topic, content, medium and tool selection in the preparation layer. To explain the components illustrated by Figure 8, the preparation layer will be linked to the iWise Mzanzi: For Schools sub-campaign introduced in the previous layer.

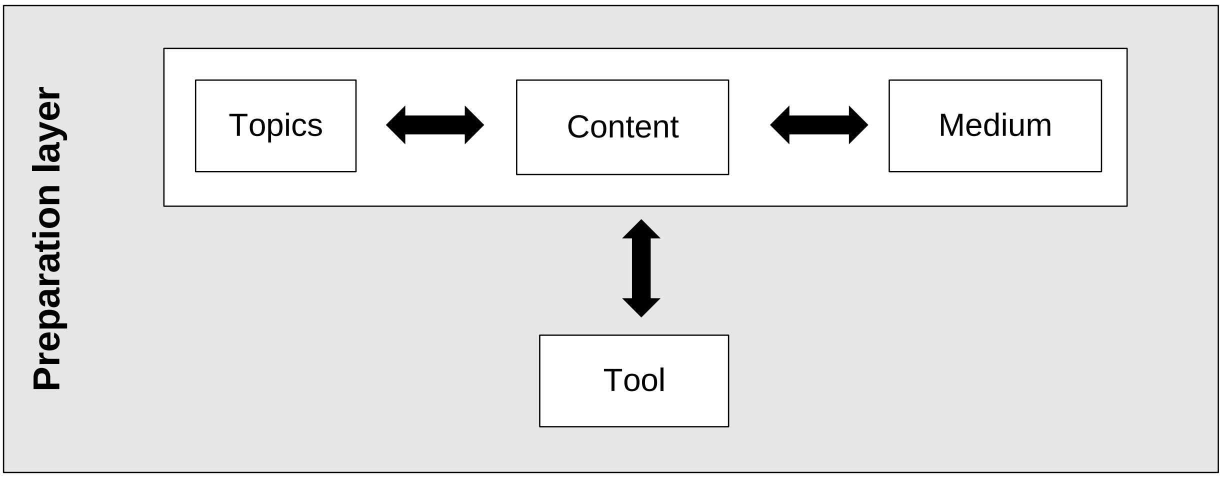


Figure 8. Preparation layer

3.5.1 iWise Mzanzi: For Schools

In South Africa the political context before 1994 led to racial inequality (Collins & Millard, 2013; Epstein, 2014) and limited skills development (Allais, 2012) — circumstances that require continued efforts to create opportunities for all citizens post-1994 (Hill, 2014; Hunter, 2015). Schools need to build an inclusive education system (Donohue & Bornman, 2014; Engelbrecht, Nel, Smit & van Deventer, 2016), improve the low standard and quality of education (Modisaotsile, 2012; Spaull, 2013), and incorporate multilingualism in teaching practices to make education accessible (Desai, 2016; Trudell, 2016).

The roll-out of electronic devices to schools, and the increasing number of children using social media tools to interact online, highlight the importance of being aware of dangers online (Sezer, Yilmaz & Yilmaz, 2015). There are several initiatives to inform children about online risks. Developing games (Giannakas, Kambourakis & Gritzalis 2015; Kritzinger, 2015; Reid & Van Niekerk, 2014a), and incorporating digital citizenship (McGillivray, McPherson, Jones & McCandlish, 2015) or cyber-safety information in the school curriculum (Von Solms & Von Solms, 2014; Walaza, Loock & Kritzinger, 2014) through subjects such as life orientation (Kritzinger, 2015) have been proposed. The development of school policies to address issues such as online bullying (Slonje, Smith & Frisén, 2013) has also received attention. These efforts are, however, hampered by context-specific and general challenges (Maringe, Masinire & Nkambule, 2015), such as limited governmental funding (Mestry & Ndhlovu, 2014) and a shortage of resources (Bayat, Louw & Rena, 2014; Modisaotsile, 2012). Schools contend with sexual harassment (Bhana, 2012), xenophobia (Hlatshwayo & Vally, 2014), homophobia

(Msibi, 2012), gender inequality (Bhana, 2015), unlawful corporal punishment (Breen, Daniels & Tomlinson, 2015; Mthanti & Mncube, 2014), high teacher absenteeism (Mashaba & Maile, 2013), and dysfunctional management, financial and staff training systems (Heyd-Metzuyanim & Graven, 2016).

South Africa has been referred to as a violent country (Shields, Nadasen & Hanneke, 2014). Violence experienced at South African schools (Smit, 2015) extends from sexual harassment (Bhana, 2012), verbal abuse (Boyes, Bowes, Cluver, Ward & Badcock, 2014) and physical attacks (Msibi, 2012), to bullying, which has also moved to the cyber world in the form of cyberbullying (Tustin, Zulu & Basson, 2014). Gangsterism (Mncube & Madikizela-Madiya, 2014), substance abuse (Waller, Gardner & Cluver, 2014), aggression (Breen, Daniels & Tomlinson, 2015), a disrespect for authority, and a decrease in discipline (Moyo, Madzima & Abdullah, 2014; Sonhera, Kritzinger & Loock, 2015), aggravates the situation. To address violence in schools, the Department of Basic Education (DBE) developed a National School Safety Framework (NSSF) to provide guidelines for school management and educators to deal effectively with issues which could lead to violence (Department of Basic Education, 2014). In the NSSF, cyberbullying is listed as one of the incidents which could lead to violence in schools (Department of Basic Education, 2014), but the framework does not address cyber-safety concerns. Schools should adopt a proactive response to cyber-safety (Jobi & Kritzinger, 2014). Importantly, although The NSSF exists, clear cyber-safety guidelines are not included. The proposed iWise Mzanzi for schools initiative focuses on creating awareness campaigns aimed at primary and secondary learners (Kortjan & Von Solms, 2014) and, with refinements, can provide the cyber-safety guidelines currently lacking in the NSSF.

The topics, content, medium and tool selection for iWise Mzanzi, will discussed in the following section.

3.5.2 Topics and content

According to Brady (2010), Internet use by children poses content, contact, conduct and security risks. Content risks refer to children having access to inappropriate or commercial information available online. Contact risks refer to children communicating and sharing personal information with unknown entities. Conduct risks include unacceptable or illegal online behaviour related to acts such as cyber bullying and piracy. Security risks refer to information security risks such as hacking, phishing, and malware, which can also affect children (Brady, 2010)

The various risks are categorised as social, physical, psychological and moral challenges (Abbasi & Manawar, 2011). Social challenges consider the effect of the Internet on the communication skills and health of children. Physical challenges refer to the interventions required to inform children about the risks of cyber use and the sedentary lifestyle which results from continuous technology use. Psychological challenges refer to mental imbalances and anti-social behaviour caused by exposure to inappropriate content. Moral challenges refer to children exposed to various information which conflicts with their religious and moral values or views (Abbasi & Manawar, 2011), and can extend to criminal activity online to further a cause (Julisch, 2013).

Children are growing up as digital citizens (Bennett, Wells & Rank, 2009; Shifrin, Brown, Hill, Jana & Flinn, 2015) with online identities (Sullivan, 2016) and participating in a digital society (Oyedemi, 2015). Digital citizens have an online or digital footprint (Daramola, 2015; Levine, 2013; Sing & Raphs, 2015) which impacts on the reputation of users permanently (Butler & Howcroft, 2014; Jones & Mitchell, 2015). The fact that children are living a digital lifestyle in an online world (Goode, 2010) requires a new approach to teaching children about safety and the responsible use of technology (Felt & Vartabedian, 2012; Ohler, 2011)—an approach that views cyber-safety and security holistically (Winn, 2012), and proposes a focus on the understanding of expectations and requirements of digital citizenship (Burridge 2010; McGillivray et al. 2015; Oyedemi, 2014).

Digital citizenship includes digital communication (Simsek & Simsek, 2013; Winn, 2012), in accordance with digital etiquette and ethics (Lindsey, 2015; Yamamoto & Ananou, 2015). It concerns digital rights and responsibilities (Sullivan, 2016), and the legal implications of online actions (Aydin, 2012; York, 2014). Digital citizenship also relates to digital health and wellness (Mossberger, 2014; Ohler, 2011), as well as digital security (Winn, 2012). Figure 9 indicates that digital citizenship education can include teaching children about civic engagement (Butler & Howcroft, 2014; Felt & Vartabedian, 2012), integrity in decision making (Furman, Theofanos, Choong & Stanton, 2012) and online respect (Broll 2014; Jones & Mitchell; 2015).

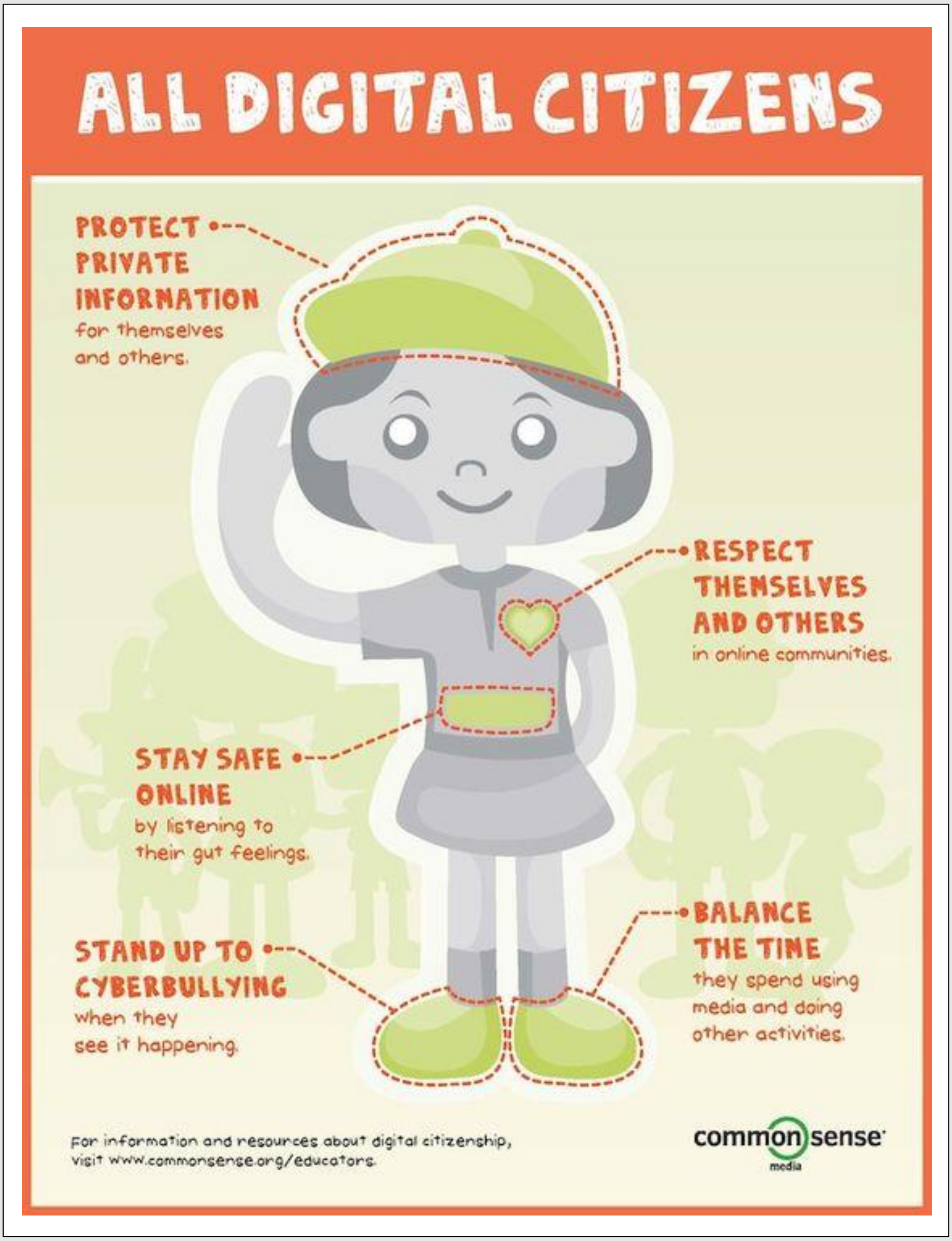

ALL DIGITAL CITIZENS
PROTECT PRIVATE INFORMATION for themselves and others.
RESPECT THEMSELVES AND OTHERS in online communities.
STAY SAFE ONLINE by listening to their gut feelings.
STAND UP TO CYBERBULLYING when they see it happening.
BALANCE THE TIME they spend using media and doing other activities.
For information and resources about digital citizenship, visit www.commonsense.org/educators.
common sense media

Figure 9. Digital citizenship (Commonsense, 2016)

The challenges or risks that accompany being a digital citizen are interlinked and form part of C3: cyber-ethics, cyber-safety and cyber-security concerns (Pruitt-Mentle, 2008; Pusey & Sadera, 2011), the range of which are itemised in Table 2.

Table 2. C3 topics (adapted from Pruitt-Mentle (2008))

Cyber-ethics	**Cyber-safety**	**Cyber-security**
• Plagiarism • Copyright • Hacking • Cyberbullying • Harassment • Fair use • File sharing • Online etiquette protocols • Posting incorrect/ inaccurate information • Stealing or pirating software, music and video • Online gambling • Gaming • Internet addiction	• Online predators • Objectionable content • Cyberstalking • Downloading • Paedophiles • Hate groups • Pornography • Unwanted communication • Online threats	• Hoaxes • Viruses and other malicious self-replicating code • Junk e-mail • Chain letters • Ponzi schemes • Get-rich-quick schemes • Scams • Criminal hackers • Hacktivists • Spyware • Adware • Malware • Trojans • Phishing • Pharming scams • Theft of identity • Spoofing • Privacy

Children need to be informed about the various aspects of cyber-ethics, cyber-safety and cyber-security with resources which are continually updated to stay current (Pruitt-Mentle, 2008; Pusey & Sadera, 2011). Cyber-ethics relates to the role of individual morals when making decisions in the cyber world (Kortjan, Von Solms & Van Niekerk, 2012; Pusey & Sadera, 2011) and acting with empathy online (Yamamoto & Ananou, 2015). Cyber-safety refers to behaviours and actions taken to minimise the risks associated with online behaviour (Pusey & Sadera, 2011). Cyber-security refers to information systems developed to protect computer hardware and software (Pusey & Sadera, 2011). These C3 topics will be discussed in the following section.

3.5.2.1 Cyber-ethics

Netiquette is a term used to describe ethical and respectful online behaviour (Butler & Howcroft, 2014; Nansen, Chakraborty, Gibbs, MacDougall & Vetere, 2012). Online etiquette training is required to ensure that computer users develop acceptable online behaviour (Ribble & Miller, 2013). Children should be taught to consider their digital identity (Broll, 2014) and the consequences of their actions (Johnson & Branson, 2012) which could lead to problems such as Internet addiction (Kalaitzaki & Birtchnell, 2014), cyberbullying (Adesote & Fatoki, 2013) and compromised online privacy due to hacking (Slusky & Partow-Navid, 2012).

The rise of Internet addiction is closely linked to three online activities (Siomos, Floros, Fisoun, Evaggelia, Farkonas, Sergentani, Lamprou & Geroukalis, 2012), gaming (Starcevic, 2013), gambling (Israelashvili, Kim & Bukobza, 2012) and pornography (Elliott & Beech, 2009). Excessive online gaming (Hussain, Williams & Griffiths, 2015) can result in gaming addiction (Goh, Bay & Chen, 2015; Ktoridou, Eteokleous & Zahariadou, 2012), which leads to behavioural problems (Rikkers, Lawrence, Hafekost & Zubrick, 2016) and the deterioration of relationships (Kim & Kim, 2015; Kuss, 2013). When accessing the Internet, children can be exposed to online gambling sites (Ciftci & Delialioglu, 2015; Vaala & Bleakley, 2015) and the risk of gambling addiction (Kuss, 2013). Internet addiction leads to difficulty in distinguishing between online and offline life (Barnard-Wills, 2012), increased cyber risks (Leung & Lee, 2012) as well as mental health (Devine & Lloyd, 2012; Siomos et al., 2012) and general health problems (Jiang & Leung, 2012). Children increasingly play online games (Walaza, Loock & Kritzinger, 2014), which has been linked to verbal aggression (Appel, Stiglbauer, Batinic & Holtz, 2014), sexism (Fox & Tang, 2014) and harassment associated with cyberbullying (Aloufi, 2015; Mark & Ratliffe, 2011).

There is an increased rate at which children experience cyberbullying (Bakar, 2015; Aboujaoude, Savage, Starcevic & Salame, 2015). Cyber- or online bullying includes trolling (Fox & Tang, 2014), displaying aggression, name-calling, threats, spreading rumours, social isolation or exclusion, intimidation, and embarrassment (Mark & Ratliffe, 2011; Vivolo-Kantor, Martell, Holland & Westby, 2014). Cyberbullying is described as a health problem (Aboujaoude et al., 2015), and victims of cyberbullying may experience anger, sadness, embarrassment, confusion and anxiety (Mark & Ratliffe, 2011) which has led to several teenage suicides (Alavi, Reshetukha & Prost, 2015). Cyberbullying often includes sharing embarrassing content about an individual (Mark & Ratliffe, 2011).

Downloading and sharing files, such as videos and photos (Omar, Daud, Hassan, Bolong & Teimmouri, 2014), can take place through social networking sites (Aladwani, 2014) and is one of the most popular uses of the Internet by children (Hamade, 2015; Nansen et al., 2012). Children can use the Internet to download movies, music, games, software and pornographic material (Kim, 2014; Tsitsika, Janikian, Schoenmakers, Tzavela, Olafsson, Wójcik, Macarie, Tzavara & Richardson, 2014). Unfortunately, children make themselves guilty of plagiarism, piracy and copyright infringement by sharing and using copyright protected material from existing websites without acknowledging the copyright owner or author (Aloufi, 2015; Hope, 2015). Piracy is linked to copyright infringement because it involves stealing, selling and distributing content owned by someone else (Kondyushova, 2014). The consequences of plagiarism, piracy and copyright infringement are seen as minimal and therefore users engage in this risky behaviour (Bardach et al., 2012). Users trust websites (Larson, 2015) and in the process of using them to download and share files or copyright-protected content illegally (Goode, 2010; Teimouri et al., 2014b), expose their devices to malicious software (Kim, 2014; Kritzinger & Von Solms, 2010). Although security software is available to protect information, hackers can access content using sophisticated hacking software (Aiken et al., 2015) and by relying on user negligence (Strawser & Joy, 2015) or user ignorance (Shava & Van Greunen, 2013). Hacking involves accessing and stealing private or confidential electronic information which belongs to someone else, without their permission and is an illegal act (Aloul, 2012; Clarke, 2015). Devices can be hacked without the user realising that it has taken place (Aiken et al., 2015) and that their privacy and safety has been compromised (Slusky & Partow-Navid, 2012).

3.5.2.2 Cyber-safety

Children need to be kept safe from inappropriate online content such as nude or semi-nude sexually explicit images and child pornography which leads to stalking, online enticement, and grooming by sexual predators (Aiken et al., 2015; Ktoridou, Eteokleous & Zahariadou, 2012; Whittle, Hamilton-Giachritsis, Beech & Collings, 2013). The term Child Abuse Material (CAM) incorporates risky sexual behaviour online (Sasson & Mesch, 2014) such as self-produced sexual materials (Aiken et al., 2015) sexting (Jones, Mitchell & Walsh, 2012; Livingstone & Görzig, 2014) and pornography (Owens et al., 2012). The risky behaviour leads to sexual harassment, and exploitation of children and adolescents (Khurana, Bleakley, Jordan & Romer, 2015).

Another major concern addressed by cyber-safety is cyberstalking. Cyberstalking involves observing (Gerson, 2013) and tracking online behaviour (Subrahmanyam, Reich, Waechter & Espinoza, 2008), often through social networking sites (Butler & Howcroft, 2014). Online stalking induces fear (Gerson, 2013), causes withdrawal from relationships or social activities and can lead to depression (Johnson & Branson, 2012). The intent of cyberstalking is to harm (Levine, 2013), harass (Burton & Leoschut, 2013; Von Solms & Von Solms, 2014; York, 2014), threaten (Smit, 2015) and initiate undesirable contact with users (Kortjan, 2013; Langos, 2014). Messages containing hate speech (O'Reilly, 2015) against individuals or groups (Teimouri et al., 2014a) to harm, harass and threaten, have legal consequences in South Africa (Smit, 2015). Hate speech includes defamatory statements made about race (Livingstone & Bulger, 2014), gender (Fox & Tang, 2014), religion and sexual orientation (Davis, Randall, Ambrose & Orand, 2015 ; Elci & Seckin, 2016). It also extends to threats of physical violence (Broll, 2014; Vanderhoven, Schellens & Valcke, 2014).

3.5.2.3 Cyber-security

Hacking can be ethical when used by companies to test the security of their cyber-security systems (Deylami, Mohaghegh, Sarrafzadeh, McCauley, Ardekani & Kingston, 2015), but is most often associated with illegal activities. Criminal hackers access and compromise sensitive data (Bendovschi, 2015) and personal information (Kondyushova, 2014; Shackelford & Fort, 2011) without authorization (Kortjan, 2013; Strawser & Joy, 2015), to commit crimes (Feng & Xie, 2014). Hackers use the information to commit fraud (Skopik, Settanni & Fiedler, 2016), steal identities (Butler & Howcroft, 2014), damage the online reputation of a user or company (Kokkinos, Antoniadou, Asdre & Voulgaridou, 2016; Tustin, Zulu & Basson, 2014), steal money (Kshetri, 2015) or obtain assets unlawfully (Abawajy, 2014). Political activism (Quigley, Burns & Stallard, 2015), ideology (Julisch, 2013), social causes (Skopik, Settanni & Fiedler, 2016) and anarchy (Quigley, Burns & Stallard, 2013) also motivate hacking attempts (Aloul, 2012) by hackers who see themselves as hacktivists (Quigley, Burns & Stallard, 2015). Hackers have hidden identities and locations (Naplavova, Ludik, Hruza & Bozek, 2014), which makes them unknown perpetrators (Aloul, 2012). They often form communities (Juszczyk, 2014), collaborate (Kajzer et al., 2014) and provide resources to assist others in hacking attempts (Johnson, 2014).

There are several methods used by hackers to obtain access to information (Aiken et al., 2015). In South Africa, phishing attempts are one of the biggest concerns for information security (Dlamini & Modise, 2012). Cyber criminals use e-mails to entice recipients to provide confidential information, by acting as legitimate senders such as financial institutions (Crompton, Thompson & Reyes, 2016). Spoofing assists in phishing attempts as legitimate names and information are used, which makes the content seem more believable (Crompton, Thompson & Reyes, 2016). Hackers can create fake websites which resemble the legitimate website of a company (Julisch, 2013), use free software downloaded by users to infiltrate a personal device (Shava & Van Greunen, 2013) or send e-mails with malicious software (Aloul, 2012). The passwords of user accounts (Johnston, Warketin & Siponen, 2015) can be used to access information illegally through a legitimate account (Choo, 2011) and are therefore targeted by hackers (McCrohan, Engel & Harvey, 2010) through malware (Crompton, Thompson & Reyes, 2016). Malware is malicious software (Bendovschi, 2015) created to infect, control, manipulate and compromise servers (Schia, 2016), systems, devices or data (Qian, Fang & Gonzalez, 2012), leave users vulnerable (Furnell & Moore, 2014). Malware includes viruses, spyware (Kondyushova, 2014), adware (Aloufi, 2015), worms (Martin & Rice, 2011) and Trojans (Labuschagne, Eloff, Veerasamy, Leenen & Mujinga, 2011). Ponzi schemes and get-rich-quick schemes (Pusey & Sadera, 2011; Sulaiman, Moideen & Moreira, 2016) can also be used to persuade unexpected victims to invest money in financial schemes (Cortes, Santamaria & Vargas, 2013) by offering a high return on investments (Greenberg & Sze, 2010). These schemes are linked to online financial crimes (Menon & Siew, 2012), which result in financial losses for investors (Lewis, 2012).

To ensure that users are safe from cyber-security threats, and act ethically online, awareness campaigns content includes cyber-ethics, cyber-safety and cyber-security topics.

3.5.3 Medium and tools

According to Kortjan and Von Solms (2014), a suitable printed or electronic medium should be selected to spread information about the topic and content selected for the campaign. The choice of medium determines the tools available to communicate with the target audience. If for example, an electronic medium is selected, video clips and websites can be used as an instrument to communicate content (Kortjan & Von Solms, 2014). Medium and tool selection will be discussed in more depth in chapter four, as it is linked to Communication Science.

3.6 Delivery layer

Figure 10 illustrates that the delivery layer, considers the target audience and defines the roles fulfilled by the audience as educator and learner (Kortjan & Von Solms, 2014).

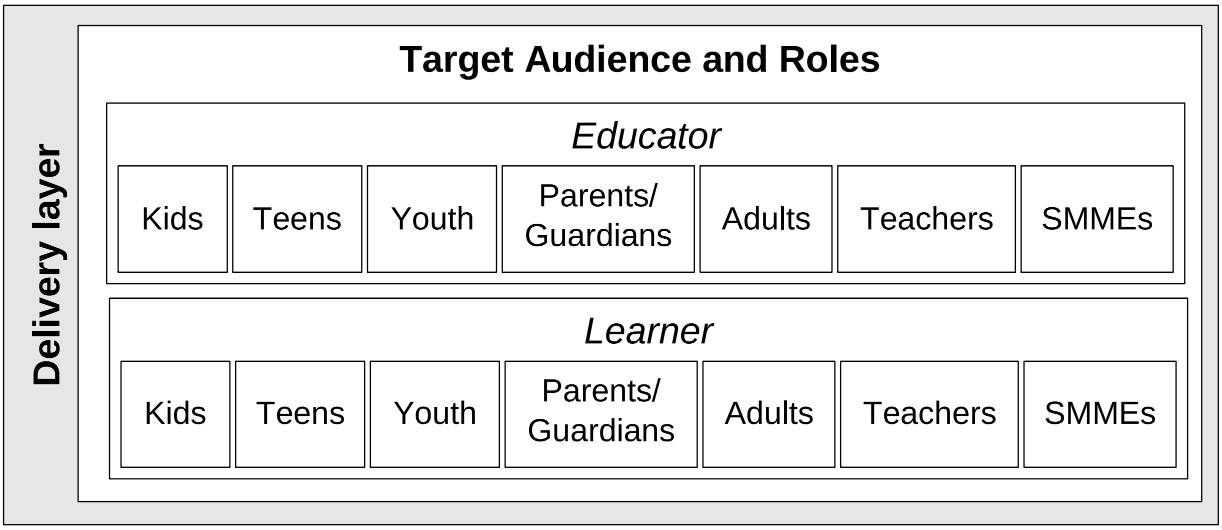


Figure 10. Delivery layer

From the audience members identified by Kortjan and Von Solms (2014), children under the age of thirteen years, teenagers, youths, parents, guardians, and teachers are relevant stakeholders for the school campaign. When trying to reach children through communication campaigns, parents and guardians need to form part of the target audience (Henley, Raffin & Caemmerer, 2011). Teachers can guide and monitor children (Mishna, Cook, Saini, Wu & MacFadden, 2011); while schools can implement cyber-safety principles and procedures (Sonhera, Kritzinger & Loock, 2015). Parents can monitor their children and enforce cyber-safe behaviour (Goh, Bay & Chen, 2015; Yusuf, Osman, Hassan & Teimoury, 2014).

3.6.1 School learners

Users currently under the age of eighteen are classified as digital natives who grew up with technology (Ktoridou, Eteokleous & Zahariadou, 2012) and are web literate (Thomas & Kielman, 2009). When these children start attending school, they may have been exposed to the cyber world as some children start using the Internet and technology before the age of five (Ktoridou, Eteokleous & Zahariadou, 2012).

3.6.2 Role of schools and teachers

Addressing cyber crimes requires a multi-level approach where the various stakeholders work together (Aiken, Mc Mahon, Haughton, O'Neill & O'Carrol, 2015). Similarly, educating children about digital citizenship requires a collaborative effort from several stakeholders (Broll, 2014; Dlamini & Modise, 2012; Livingstone, Davidson, Bryce, Millwood Hargrave & Grove-Hills, 2011), including government (Buono, 2014), parents (Rudi, Dworkin, Walker & Doty, 2014), teachers (Sezer, Yilmaz & Yilmaz, 2015), schools (Zhu, Zhang, Yu & Bao, 2015), social workers (Martin & Slane, 2015), law enforcement (Davis, 2012), the information technology industry (Livingstone et al., 2011), Internet service providers, and non-profit organisations (Aloul, 2012). The NSSF also proposes collaboration of stakeholders, which includes the school principal, school safety committee, parents, learners, educators, school governing bodies, student bodies, community actors, other school staff and school structures. Safety is used as an umbrella term in the NSSF, and there is a strong focus on collaborating with different stakeholders to combat the problems associated with safety at schools (Department of Basic Education, 2014).

Safety efforts at schools should include prevention (Al-karaki, Harous, Al-muhairi, Alhammadi, Ayyoub, Alzaabi, Alsalhi, Salem & Alamiri, 2016; Barnard-Wills, 2012), protection (Bovina, Dvoryanchikov & Budykin, 2014) and support practices (Myers, Haworth & Hayton, 2016) to mitigate the likelihood of potential problems. The involvement and support of teachers and parents influence the effectiveness of any awareness campaign aimed at children (Jarvis, Rhodes, Deshpande, Berry, Chulak-Bozzer, Faulkner, Spence, Tremblay & Latimer-Cheung, 2014). Schools or educational centres can contribute to successful intervention programmes targeting the youth (Kritzinger & Padayachee, 2013); and teachers can have a positive influence on the behaviour of learners (Lozano, Prades & Montagut, 2015).

Studies have shown that some school teachers may not have the knowledge required to support students who encounter problems associated with the use of online platforms (Görzig & Ólafsson, 2013; Sezer, Yilmaz & Yilmaz, 2015; Slonje, Smith & Frisén, 2013). Although teachers are encouraged to make use of technology in their teaching practices, they are not always adequately prepared to deal with and teach cyber-safety basics (Ktoridou, Eteokleous & Zahariadou, 2012; Pusey & Sadera, 2011). In addition, teachers may feel threatened when learners display more ICT knowledge than they themselves have (Moyo, Madzima & Abdullah, 2014). Even though some teachers have the skills required to use ICT, they may not have the knowledge needed to use it for educational purposes (Moyo, Madzima & Abdullah, 2014). New teachers, therefore, need to receive cyber-safety training as part of their qualifications (Ktoridou, Eteokleous & Zahariadou, 2012). Moreover, schools have an obligation to educate teachers and parents about the strategies required to keep children safe, and to inform them about the legal consequences of online behaviour, such as cyberbullying (Mark & Ratliffe, 2011). However, although there are schools in South Africa who have developed appropriate cyber policies (Collegiate High School Governing Body, 2016), most schools do not have cyber policies in place (Hope, 2015) and lack the knowledge or skills required to protect the online privacy of learners (Clemons & Wilson, 2015). Moreover, the integration of technology in the classroom is hampered by inaccessible ICT resources and equipment, and negative personal perceptions and attitudes towards incorporating technology in the classroom (Moyo, Madzima & Abdullah, 2014).

3.6.3 Role of parents or guardians

According to (Ktoridou, Eteokleous & Zahariadou, 2012), cyber-safety risk awareness should form part of family values. When trying to reach children, communication with parents should also be facilitated (Ridley, 2015) as children often take on the attitudes of their parents (Kim & Kim, 2015). Parents need to discuss the roles and responsibilities of a digital citizen with their children (Livingstone et al., 2011), to work with schools and teachers (Mark & Ratliffe, 2011). Parents and adults who fulfil a supervision role need to monitor children's use of the Internet and impose restrictions to ensure that they are safe (Hill, 2015; Ktoridou, Eteokleous & Zahariadou, 2012). Parents and guardians also need to be alert for warning signs and intervene to minimise the emotional impact associated with issues such as cyberbullying and understand how a child experiences these problems (Ktoridou, Eteokleous & Zahariadou, 2012). Monitoring is important during the adolescent years as a conflict between parents and teenagers can lead to children immersing themselves in the cyber world and forming relationships online with strangers (Kim & Kim, 2015). Monitoring online activity can, however, be challenging as parents are not aware of all the risks associated with the cyber world; and, as the instances of online bullying amongst children increase, the need for interventions becomes increasingly important (Kennison & Read, 2003; Ktoridou, Eteokleous & Zahariadou, 2012). Monitoring is also challenging because children feel that they have the right to privacy (O'Reilly, 2015) which is often supported by legislation (Devine & Lloyd, 2012).

Once the target audience has been identified and defined in the preparation layer, the campaign is implemented (Kortjan & Von Solms, 2014).

3.7 Monitoring layer

The final layer in the framework is concerned with an evaluation to determine how effective initiatives are. Figure 11 indicates that benchmarking, success indicators and periodic status reports are required for the evaluation process.

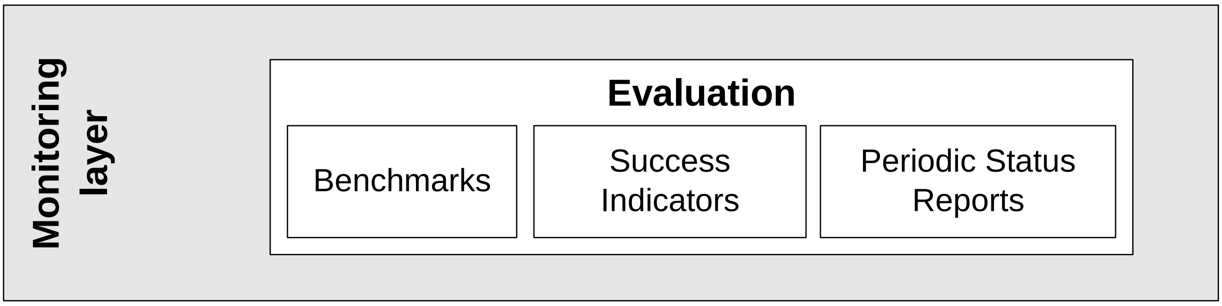


Figure 11. Monitoring layer

Periodic status reports allow for the monitoring of success indicators and assist campaign planners to benchmark (Kortjan & Von Solms, 2014). Benchmarking refers to setting standards or guidelines based on good practice (Cronjé & Van Wyk, 2013). The guidelines assists future initiatives to conform to the set standard (Verbeke & Tung, 2013) and should be maintained and updated continuously (Čábyová & Ptačin, 2014). Benchmarking uses the results of success indicators or key performance indicators (KPIs) to identify good practice (Rantos, Fysarakis & Manifavas, 2012). The KPI's andmetrics used to measure success, depends on campaign or program objectives and the activities implemented to meet the objectives. Popular metrics include campaign reach and the frequency of exposure to campaign messages (Groeger & Buttle, 2014) The results of the assessment are reverted to considerations at the tactical layer/stage to determine whether any changes are required for future campaigns (Kortjan & Von Solms, 2014).

3.8 Conclusion

Chapter three discussed the five-layer cyber-security awareness and education framework developed by (Kortjan & Von Solms, 2014). The framework has not been implemented and therefore, the discussion in chapter three has largely focussed on what should be included in the strategic, tactical, preparation, delivery, and monitoring layers, based on the study by (Kortjan, 2013) and relevant information technology literature.

The framework proposes a national campaign called iWise Mzanzi, which consists of a national awareness week; a community outreach programme; a campaign for all citizens; and a campaign aimed at schools. The iWise Mzanzi: For Schools campaign is used to illustrate how awareness campaigns are planned and attention is placed on the preparation and delivery layers of the framework. The preparation layer contains topics, content, medium and tool selection. According to the literature reviewed in chapter three, campaign topics and content need to focus on cyber-security, cyber-safety and cyber-ethics, which forms part of digital citizenship. The medium used to deliver the key campaign messages should be aligned to the tools selected. The delivery layer requires campaign planners to select the intended recipients and defining the roles played by the audience. Reaching the intended audience requires a clear description of who the target audience is and how the individual members fulfil the roles of learner and educator. Chapter three discussed the development of campaigns from an information technology experience and chapter four will discuss the elements required for campaigns, as identified in communication theory.

CHAPTER 4 CAMPAIGN PLANNING

“I almost wish I hadn’t gone down that rabbit-hole—and yet, it’s rather curious.”

(Lewis Carroll, Alice's Adventures in Wonderland)

Entry vignette Abstract		
Introduction to case and context Chapter one: Introduction **Research question:** What are the elements required for the preparation and delivery of a cyber-safety awareness campaign?		
Chapter two: Research methodology		
Research objective I. To identify, using existing literature, the essential elements required for conducting a cyber-safety awareness campaign in South Africa.	**Description of case and context**	
	Chapter three: Cyber-safety in South Africa	Chapter four: Campaign planning
	Information Technology perspective	*Communication Science perspective*
Research objective II. To describe an existing South African cyber-safety awareness campaign aimed at schools, which forms the single case study;	**Development and detail about selected of issues** Chapter five: SACSAA campaign	
Research objective III. To compare the case study with the identified elements, and to determine whether there are any application gaps and areas for improvement;		
Research objective IV. To make recommendations for improved and integrated strategies for cyber awareness campaigns in South Africa.	**Lessons learnt and closing vignette** Chapter six: Conclusion Findings and recommendations	

4.1 Introduction

Communication campaigns are planned efforts or messages sent to audiences with the intent to meet specific outcomes within a pre-determined time frame (Werder, 2015). The intended outcome linked to campaigns often involve behaviour change (Nathanail & Adamos, 2013) achieved through the use of persuasive message appeals (Guttman, 2015). Planning campaigns is a complex process, which contains several processes and steps to consider (Henley, Raffin & Caemmerer, 2011). According to Rice and Atkin (2013), there is no encompassing theory for campaign planning and therefore, six popular models are discussed in chapter four to identify the elements required for campaign planning from a Communication Science perspective.

4.2 Campaign planning approaches

A review of the literature has led to the identification of six models, or frameworks, used for campaign planning. The basic features of each of these approaches are summarised in Table 3.

The first approach refers to the campaign principles proposed by Wilcox and Cameron (2014). The principles contain seven stages and were developed for public relations campaigns. The second program and campaign planning framework, developed by Cornelissen (2014), consists of six stages and was developed for communication campaigns. The third approach, suggested by Perloff (2014), is used for social marketing campaign planning and has five stages. Social marketing applies marketing principles to campaigns promoting some form of social change in society (Kubacki et al., 2015; Lefebvre, 2013). The fourth approach refers to The Public Relations Institute of Southern Africa's seven steps for programme planning (Skinner, Mersham & Benecke, 2013). The fifth approach contains the planning stages for public relations campaigns summarised by Gregory (2010). The sixth approach considers the steps required for the development of effective communication campaigns proposed by Kotler, Armstrong and Tait (2010).

Table 3. Campaign Planning

Planning stages	Campaign principles (Wilcox & Cameron, 2014)	Program and campaign planning framework (Cornelissen, 2014)	Social marketing campaign planning steps (Perloff, 2014)	PRISA 7 Step programme (Skinner, Mersham & Benecke, 2013)	Comprehensive planning tool (Gregory, 2010)	Steps in developing effective communication (Kotler, Armstrong & Tait, 2010)
Stage one	Situation analysis	Strategic intent	Planning (campaign objectives)	Situation analysis	Situational analysis • Organisation’s societal and/or corporate objectives • Issues that threaten or provide an opportunity for realising those objectives • Public relation’s contribution defined	Identify the target audience
Stage two	Objectives • Informational/ educational objective • Motivational objective	Define communication objectives	Select theories relevant to campaign objectives to support campaign strategies	Formulating campaign objectives	Strategy • PR aim(s) and objectives • Stakeholders/ public involved and content of programme • Strategy	Determine the communication objectives

Table 3. Campaign Planning (Continued)

Planning stages	**Campaign principles (Wilcox & Cameron, 2014)**	**Program and campaign planning framework (Cornelissen, 2014)**	**Social marketing campaign planning steps (Perloff, 2014)**	**PRISA 7 Step programme (Skinner, Mersham & Benecke, 2013)**	**Comprehensive planning tool (Gregory, 2010)**	**Steps in developing effective communication (Kotler, Armstrong & Tait, 2010)**
Stage three	Target audience • Primary audience • Secondary audience • Tertiary audience	Identify and prioritise target audiences	Communication analysis • Audience analysis and segmentation • Research to determine audience perceptions • Channel analysis and selection	Identifying target publics	Implementation Tactical programme with timescales and resources allocated	Design a message
Stage four	Overall campaign strategy	Identify themed message(s)	Campaign design and implementation	Formulating message	Evaluation	Choose media through which to send message
Stage five	Tactics required to implement strategy	Develop message styles	Evaluation and reorientation	Implementing actions		Select message source
Stage six	Calendar/ Timetable	Develop a media strategy		Draw up a budget		
Stage seven	Conducting an evaluation			Evaluation		

4.3 Stage 1: Situational Analysis

Wilcox and Cameron (2014), Skinner, Mersham and Benecke (2013) and Gregory (2010) refer to situational analysis as the first step in campaign planning. A situational analysis determines the purpose, scope, and maturity of the campaign (Dorfman, Ervice & Woodruff, 2002), where purpose refers to the strategic intent of the initiatives, scope refers to the extent of the campaign, and maturity relates to the existing resources allocated to address the issue of concern (Werder, 2015). Cornelissen (2014) refers to strategic intent as the first part of campaign planning, which is seen as one of the elements of situational analysis. Maturity refers to the level of development of both the campaign and the issue it addresses (Gregory, 2010). A SWOT analysis, which considers the internal strengths and weaknesses of a project or organisation to identify opportunities and threats external to the project or organisation (Monzani et al., 2014), can be used to determine the maturity of a campaign The analysis takes into consideration corporate objectives and the issues which affect attaining those objectives.

For campaigns to be successful, the strategic intent or purpose of the campaign should be clearly defined, and the target audience should be identified to determine the scope or reach of the campaign (Werder, 2015). Gregory (2010) identifies target audiences as part of the situational analysis during stage one. Kotler, Armstrong and Tait (2010) also identifies target audiences during the first stage, but, for the present study planning a cyber-security campaign will start with conducting a situational analysis to provide a context for the campaign and to assist in determining holistically the purpose, scope and extent of the campaign. If the campaign starts with identifying the target audience, important considerations which will influence campaign success may be left out. Identifying the target audience will, however, be moved to stage two of cyber campaign planning.

4.4 Stage 2: Identify the target audience

Although Wilcox and Cameron (2014), Cornelissen (2014), Perloff (2014), and Skinner, Mersham and Benecke (2013) identify the target audience during the third stage of campaign planning, knowing who the audience is before the start of stage three will assist in developing communication objectives which address the purpose identified during the situational analysis (stage one) so as to attend to the needs of the intended audience.

Market segmentation is a marketing concept which refers to selecting a specific audience for communication (Dooley, Jones & Iverson, 2012). Selecting a broad general public creates challenges for campaign planners, as stakeholders have different needs, wants and interests (Chapleo, 2010; Howitt & McManus, 2012). Segmentation therefore divides the target audience into smaller groups (Bock, Poole & Joseph, 2014; Kubacki et al., 2015), based on biographical or psychographic information (Dooley, Jones & Iverson, 2012; Ekos Research Associates, 2011; Miller, 2010). A detailed stakeholder analysis is required to identify who the stakeholders are and to describe clearly what their needs and expectations are within their existing frame of reference and the context they function in (Laczniak & Murphy, 2012).

It is challenging to determine how much information the intended audience has about a topic before encountering the campaign message (Averbeck, Jones & Robertson, 2011). Research is therefore required during the process to identify the target audience and their needs (Singh, 2012).

4.5 Stage 3: Determine the communication objectives and resources allocated

Campaign goals or objectives (Fraustino & Ma, 2015) should adhere to the principles of SMARTA; namely to be specific, measurable, attainable, realistic, time-bound and adjustable. According to (Willis et al., 2013), communication campaigns intend to educate, inform, recall, remind, provide support, and facilitate communication and decision making. Objectives in the case of cyber usage can include raising awareness (Rantos, Fysarakis & Manifavas, 2012) and reducing or changing behaviours (Page & Sharp, 2012), to identifying interventions and creating partnerships with parents or guardians (Saladin-Subero & Hawkins, 2011).

Wilcox and Cameron (2014), Cornelissen (2014), Perloff (2014), Skinner, Mersham and Benecke (2013) and Gregory (2010) develop communication objectives during the second stage of campaign planning. It is fair, then, to ask why communication objectives are moved to stage three for cyber campaign planning when other planning models list it as stage two. Five of the six approaches contained in Table 3 are used to sell products, services or experiences through marketing, public relations or communication campaigns. For these purposes, campaign objectives can be developed before defining the intended audience as they are often linked to generic intentions, such as improving sales figures. With cyber-security campaigns, the main objectives will be to inform and educate the intended audience about C3 topics. According to Ridley (2015), audience participation is important for campaign success. Knowing the intended audience before setting the objectives, will allow the campaign planner to move from generic, broad campaign objectives, to more targeted objectives which address the specific needs of the audience.

Communication objectives can be limited by the range of resources available to campaign planners. Resources range from funding to the skills required to plan and implement the campaign. Budget constraints can, for instance, influence the selection of communication mediums used (Mulhern, 2009). It is, therefore, important to consider whether resources are available when developing communication objectives.

4.6 Stage 4: Formulate a communication strategy

Wilcox and Cameron (2014) develop a communication strategy during Stage Four and choose tactics to implement the strategy in Stage Five. During Stage Four, Skinner, Mersham and Benecke (2013) refers to message formulation, and Cornelissen (2014) emphasises the development of message themes and designs. Once the communication objectives have been developed (in Stage Three), Stage Four requires a strategy which successfully integrates tools and techniques associated with the fields of marketing, public relations, advertising, branding and design, to develop an effective message. An integrated approach combines elements from the marketing mix and communication mix (Barker, 2013). Integration is necessary because it leads to coherence and consistency in the messages designed and increases the credibility of the campaign (Johansen & Andersen, 2012).

Figure 12 illustrates that the communication mix refers to a combination of advertising, public relations, personal selling and sales promotion to compile a communication plan used to communicate with a target market or target audience (Barker, 2013; Lamb, Hair, McDaniel, Boshoff, Terblanche, Elliott & Klopper, 2015; Singh, 2012). Advertising presents information to a target audience in a compelling manner, while personal selling is a personal presentation of information to a target audience (Šramová, 2015b). Public relations refers to building mutually beneficial relationships with the major stakeholders

(Estanyol, 2012). Direct marketing is targeting special deals or promotions to an audience (Šramová, 2015b).

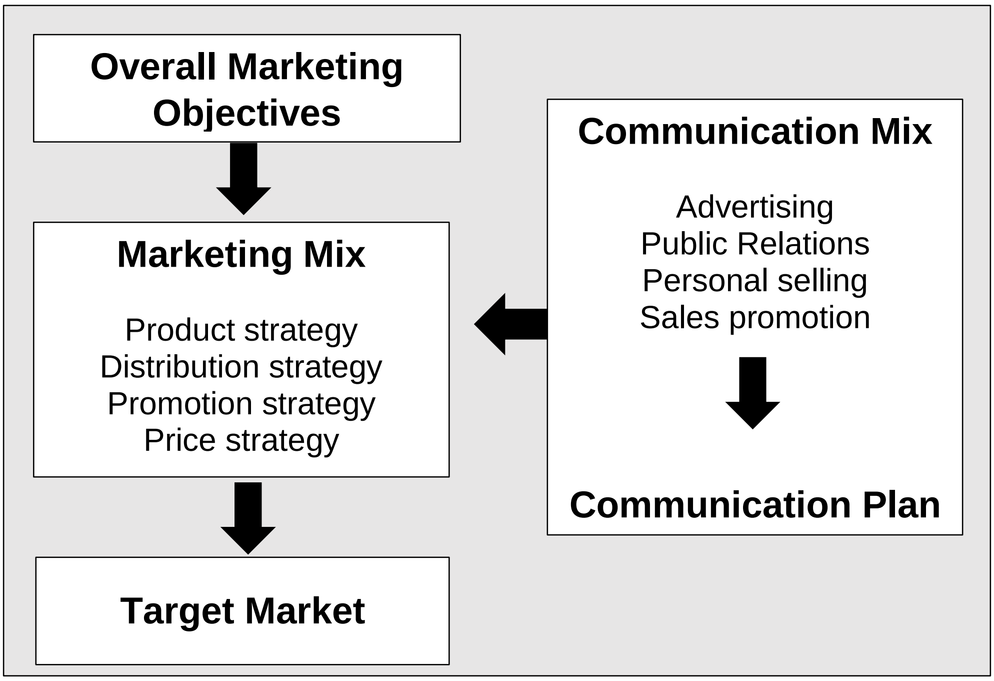


Figure 12. The marketing and communication mix
(Adapted from Lamb, Hair, McDaniel, Boshoff, Terblanche, Elliott & Klopper, 2015)

The marketing mix refers to the product, distribution, promotion and price strategy used to sell a product or service to potential clients (Kubacki et al., 2015; Raval, Tanna & Raval, 2014). Although the marketing mix elements are applied when developing strategies to market tangible products (Idris & Whitfield, 2014; Kubacki et al., 2015), the elements can also be employed in communication campaigns. The marketing mix considers the development of products and services, how they will be distributed, which promotional tools will be used to market the product and which pricing strategy would be most suitable (Goi, 2009). The product would be the main ideas to promote (Henley, Raffin & Caemmerer, 2011), which, in the context of C3, would be cyber-ethics, cyber-safety and cyber-security. The product in this case refers to the underlying advantage of being aware (Henley, Raffin & Caemmerer, 2011) of cyber risks and acting responsibly online. Place refers to where cyber-safety information is made available and whether there are any partners or intermediaries to assist with the distribution of content (Henley, Raffin & Caemmerer, 2011). Price considers the financial and non-financial costs and benefits involved in obtaining information and changing behaviour, as suggested by the campaign (Kubacki et al., 2015). Promotion refers to the activities and tools used to create awareness about the campaign. Tools from the advertising, personal selling, sales promotion or public relations fields are selected according to the goal of the campaign, the preference of the target audience and available budget (Henley, Raffin & Caemmerer, 2011).

Kotler, Armstrong and Tait (2010) design a message during Stage Three, select the medium to send the message through in Stage four, and select a message source in Stage Five. When developing a message, it is important to know which medium will be used as it influences how the message will be presented. To ensure that message recipients view the campaign content as credible, the message source should be selected carefully when developing the message. These decisions are interdependent, and are therefore included in stage four of campaign planning as sub-categories. A campaign planner would first select the communication medium, then develop the message to suit the medium, and finally, construct an implementation plan. If more than one medium is used for the campaign, the same key message will be utilised for all campaign material to ensure consistency, but the way in which the message is presented, might be different to accommodate the requirements of the mediums (Saeed, Naeem, Bilal & Naz, 2013)

The sub-categories of stage four will be discussed in the following section.

4.6.1 Selecting the communication medium

Selecting the correct medium and media channel to communicate a message is essential to get a message across to the identified audience (Muda, Musa & Putit, 2012). The tactics mentioned by Wilcox and Cameron (2014), would therefore form part of media channel selection, which forms part of Stage Five in the framework proposed by Kotler, Armstrong and Tait (2010). The channel used to communicate with the target audience, will influence the design elements required to convey the campaign message.

Popular media or communication channels used by integrated campaigns include newspapers, magazines, radio, television, outdoor media and the Internet (Kotler, Armstrong & Tait, 2010). Newspapers and magazines serves the purpose of providing factual, informative or educational information to readers (Kumari, 2014). The print publications offer paid-for advertising space, but publicity can also be obtained by offering newsworthy articles relating to the campaign (Tallapragada, Misaras, Burke & Waters, 2012). Advertising space can be bought on radio and television or public service announcements can be distributed to the channels in an attempt to receive on-air exposure (James, Albrecht, Litchfield & Weishaar, 2013). Outdoor media takes the form of paid-for billboards placed outside for passing traffic or pedestrians to see (Beneke, 2011). Social media are used extensively for online campaigns as it is interactive and facilitates a dialogue with message recipients (Fraustino & Ma, 2015). Channels are selected according to campaign objectives and the characteristics, advantages and limitations of each media type (Mulhern, 2009; Simsek & Simsek, 2013).

For campaigns aimed at children, alternative methods such as posters, magnets (James et al., 2013), advertising in school newsletters or publications and in-school presentations have been used (Beneke, 2011).

4.6.2 Design a message

During stage four, Skinner, Mersham and Benecke (2013) refers to message formulation, and Cornelissen (2014) emphasises the development of message themes and designs. Campaign planners need to develop the message content and structure (Kotler, Armstrong & Tait, 2010) and integrate creative design elements to enhance synergy and effectiveness (Mulhern, 2009; Smith, 2012).

Communication design processes enhance interventions or campaigns (Harrison, 2014). Visualisation should be used to present information in a creative, meaningful way (Lavigne & Gouin, 2014), but the intended message is not always transmitted and understood as planned (Epure, Eisenstat & Dinu, 2014). Situational and cultural context play a critical role in meaning-making (Boeriis & Holsanova, 2012) for the target audience and therefore influence the design elements used.

For printed content, copy, images and colour choices would be necessary. For radio content, word, sound and voice selection would be made, while broadcasted messages for mediums such as YouTube or TV would consider non-verbal communication (Kotler, Armstrong & Tait, 2010). Communication as design considers the development and evaluation of messages (Barbour & Gill, 2014). The design of messages is context-specific and, as such, general principles of design can guide the process of development (although they may not apply to all contexts) (Harrison, 2014). Formative research is required to obtain data which will assist the campaign planner in designing messages which appeal to the target audience (Henley, Raffin & Caemmerer, 2011).

All messages should adhere to the principles of AIDA (Antonova, 2015)—the acronym for Attention, Interest, Desire and Action—used to explain the process which the target audience should go through in a communication exchange (Rawal, 2013). The campaign needs to attract the attention of the target audience, maintain interest, stimulate the desire to comply with what the campaign message suggests and to act on the message (Rawal, 2013). Thus, audience members need to attend to the content of the campaign (Averbeck, Jones & Robertson, 2011), which should be easy to understand and act upon (Henley, Raffin & Caemmerer, 2011).

Eye-catching design elements, such as conflicting colours (Lavigne & Gouin, 2014; O'Connor, 2015), bright colours and large font can be used to arrest the attention of the target audience (Domigan, Glassman & Miller, 2015). Although not all colours have universal meanings and are often influenced by cultural contexts (Berehoiu, Wohlfarth & Sam, 2013), colour psychology is important in material design. Perceptions and emotions (Andersen, Vuori & Guillaume, 2015; Dael, Perseguers, Marchand, Antonietti & Mohr, 2015) are subconsciously linked to colour (Hanafy & Sanad, 2015; Ünal, 2015). The colour red, for instance, has implicitly been used in campaigns to signify danger (Pravossoudovitch, Cury, Young & Elliot, 2014). Colours have significations attached by the target audience and can, therefore, contribute towards the meaning of a message (Andersen et al., 2015). Colour selection has been found to influence the response of children to campaign messages (Mohebbi, 2014).

Message framing is used to make print and broadcast campaign material more persuasive and revolves around the idea of using message appeals to create the desire to act (Yan, Dillard & Shen, 2012). Message appeals are developed as part of a creative concept to interest the target audience (Akbari, 2015). Framing includes positive emotional appeals, such as humour or hope (Chadwick, 2014), to negative emotional appeals, such as fear (Ferguson & Phau, 2013) or threats (Charry & Demoulin, 2012). Emotional appeals can contribute to information recall (Kim & Kiousis, 2012), while the use of moral appeals, such as sympathy (Kemp, Kennett-Hensel & Kees, 2013), contribute to the support of a cause. Appeals to reason use logical arguments and explanations to persuade audience members to change their behaviour (Guttman, 2015).

All message design elements need to be developed, integrated and aligned (Illia, 2012) consistently with the branding created for the organisation, campaign organiser or campaign (Toledano, 2010). Brands create an identity (Halliburton, 2012), association (Mann & Ghuman, 2015) or value (Hamzah, Syed Alwi & Othman, 2014) for organisations, products or services. A combination of design elements (Bastos & Levy, 2012), logos (Blombäck & Ramírez-Pasillas, 2012), images (Bastos & Levy, 2012), symbols (Chapleo, 2010), slogans, promises (Balmer, 2012; Chung, Lee & Heath, 2013) typeface selection, and colour use are used to elicit responses from a target audience (Freeman, Harrison, Wicks, Parmar & Colle 2010; Koll & Von Wallpach, 2014) and build loyalty (Pinar, Trapp, Girard & Boyt, 2011). The credibility of a campaign is considered when developing the message (Vlăduțescu, 2013). Decisions such as whether to draw clear conclusions or to leave it to the audience, and when to present the strongest arguments, impact on the credibility of campaign material (Kotler, Armstrong & Tait, 2010). There are conflicting results of research on the importance placed on the credibility of the source in a campaign (Fisher, Magee & Mohammed-Baksh, 2015), but how the target audience views the communicator may affect the perceived credibility of the information (Clark, Wegener, Sawicki, Petty & Briñol, 2013; Smith, 2013). Credibility is often linked to the perceived trustworthiness, expertise, and enthusiasm of the sender (Lowry, Wilson & Haig, 2015) or brand (Ewing, 2009). Trust is a major factor in brand communication (Laroche, Habibi & Richard, 2013).

Brands develop over time (Vernuccio, 2014). Companies often use celebrities for endorsements to build loyalty for a brand (Hollensen & Schimmelpfennig, 2013; Šramová, 2015b). Endorsers can take the form of brand characters or mascots (Hosany, Prayag, Martin & Lee, 2013), which attract the attention of children especially (Patterson, Khogeer & Hodgson, 2013) and can become akin to celebrities (Pairoa & Arunrangsiwed, 2016). Figure 13 provides examples of three sets of mascots developed for cyber-safety campaigns for children and include Hippo and Hedgehog (Palmieri, 2016), the Privacy Pirates (MediaSmarts, n.d.), as well as Hector the dolphin (Hector's World Limited, n.d.).

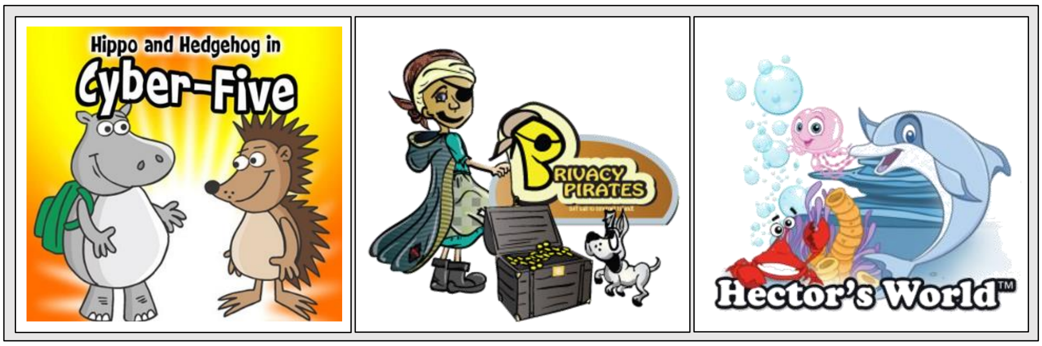


Figure 13. Animated characters for cyber campaigns
(Palmieri, n.d.; MediaSmarts, n.d.; Hector's World Limited, n.d.)

Once the message design aspects (such as message content, structure, format and the source, which lends credibility to the information) have been established, the campaign implementation must be planned. Implementation includes the different tools and mediums used to present the information and the choice of strategy (information, response, or involvement) made to allow effective communication with stakeholders.

An information strategy making use of one-way communication is used to convey information to a target audience (Walter, 2014). When attempting to create a dialogue about particular issues of concern, or to change the attitude or behaviour of stakeholders, the response strategy would be suitable as it adopts a two-way communication—as proposed by Grunig and Hunt's two-way symmetric model of communication (Cornelissen, 2014). The involvement strategy approach to communication extends the response/dialogue approach to active collaboration by stakeholders, to allow stakeholders to contribute towards decision-making processes (Walter, 2014). Although the target audience may not be communication specialists, their feedback regarding the campaign can lead to improvement of initiatives (Domigan, Glassman & Miller, 2015) and the roles played by stakeholders should therefore be considered when planning the implementation of campaigns (Vaala & Bleakley, 2015).

4.6.3 Implementation plan

Communication campaigns require resources, such as financial investment and human participation, which makes it necessary to set a specific time allocation for the activities linked to the campaign. Both extensive campaigns and small campaigns on a limited budget can be used to communicate with target audiences (Dorfman, Ervice & Woodruff, 2002). When developing the implementation plan, the roles played by stakeholders in processing and sharing the key message should be considered (Broll, 2014; Skopik, Settanni & Fiedler, 2016), as collaboration from the target audience contributes to campaign success (Martin & Rice, 2011). After selecting the tactics required to implement the campaign strategy, Wilcox and Cameron (2014) refer to a calendar or timeline and PRISA considers budget implications. The implementation strategy, therefore, finalises the budget and plans the appropriate timing for activities aimed at a specific target audience (Walter, 2014).

4.7 Stage 5: Evaluation

Implementation is followed by an evaluation to measure campaign success (Saeed et al., 2013). Wilcox and Cameron (2014), Perloff (2014), Skinner, Mersham and Benecke (2013), and Gregory (2010) refer to evaluation as the final stage of campaign planning. Campaigns are evaluated to determine whether it was effective (Henley, Raffin & Caemmerer, 2011), to test message recall (James, 2011), to confirm whether the message was processed as intended (Ewing, 2009), to establish whether the most appropriate channels of communication was used (Reinold & Tropp, 2012), and to confirm whether the campaign led to behaviour change (Johnston, Warkentin & Siponen, 2013).

Cyber-safety is an ongoing awareness effort, and therefore campaigns must be monitored and evaluated continuously (Rantos, Fysarakis & Manifavas, 2012). According to Watson (2012), campaign results need to be aligned to the set objectives and effective campaign strategies must be documented. Based on the effectiveness of campaigns, adjustments or corrections (Rantos, Fysarakis & Manifavas, 2012) and benchmarks (Čábyová & Ptačin, 2014) can be proposed for future initiatives.

During the final stage, a campaign planner must monitor, evaluate and report on the effectiveness of initiatives to identify campaign elements which requires adjustment to contribute to further campaign success. Evaluation often involves obtaining feedback form the target audience (Diga, Nwaiwu & Plantinga, 2013) and stakeholders are therefore part of stage five.

4.8 Conclusion

Chapter Four considered six communication models used for campaign planning. These had a range of frameworks setting out the order in which the various activities should be addressed.

According to Wilcox and Cameron (2014), campaign planning starts with a situational analysis, followed by setting objectives, identifying the target audience, developing an overall campaign strategy, selecting tactics to implement the strategy, and developing a calendar to track implementation. The final stage ends with evaluating campaign success. In the second model, Cornelissen (2014) starts with determining the strategic intent of the campaign, followed by developing communication objectives. In contrast to the other models, Cornelissen (2014) identifies and prioritises target audiences, and develops themed message(s), message styles and a media strategy. For the third model, Perloff (2014) develops campaign objectives and selects theories relevant to campaign objectives to support campaign strategies. Perloff (2014) suggests conducting a communication analysis, which includes an audience analysis and segmentation, research to determine audience perceptions, and channel analysis and selection. The communication analysis is followed by campaign design, implementation, and evaluation. The fourth model, promoted by Skinner, Mersham and Benecke (2013), considers seven steps, starting with a situational analysis, and formulating campaign objectives. Once the target public is identified, a message to reach the intended audience and campaign implementation are planned, followed by a budget review. After campaign implementation, evaluation follows. Gregory (2010), in the fifth model considered, refers to situational analysis, strategy, implementation and evaluation of the four main stages of campaign planning. Finally, Kotler, Armstrong and Tait (2010) start with identifying the target audience and determining the communication objectives. Next, a message is designed, and media through which to send the message and the message source are selected.

Although the six approaches vary in the number of planning stages and the order in which the stages are executed, the core elements required for campaign planning are shared by these models- namely:

- A purpose
- Target audience
- Objectives
- Campaign strategy
- A message
- Medium or channel to convey the message
- Implementation
- Evaluation

The campaign planner should establish the purpose or strategic intent of the campaign by conducting a situational analysis. Next, the target audience should be identified to ensure that communication objectives are targeted at the needs of the intended audience. Once communication objectives are set, the campaign requires an overall strategy to guide message channel selection, message design elements and an implementation plan to execute the campaign successfully. Once the campaign has been implemented, monitoring and adjustment are required to evaluate and report campaign progress.

The five stages can be further allocated to the preparation and delivery layer of the cyber-security awareness and education framework as illustrated by Figure 14. All the stages required to develop the campaign, are placed in the preparation layer. The delivery layer contains the implementation stage, which includes monitoring and reporting on campaign progress and adjustments made during execution.

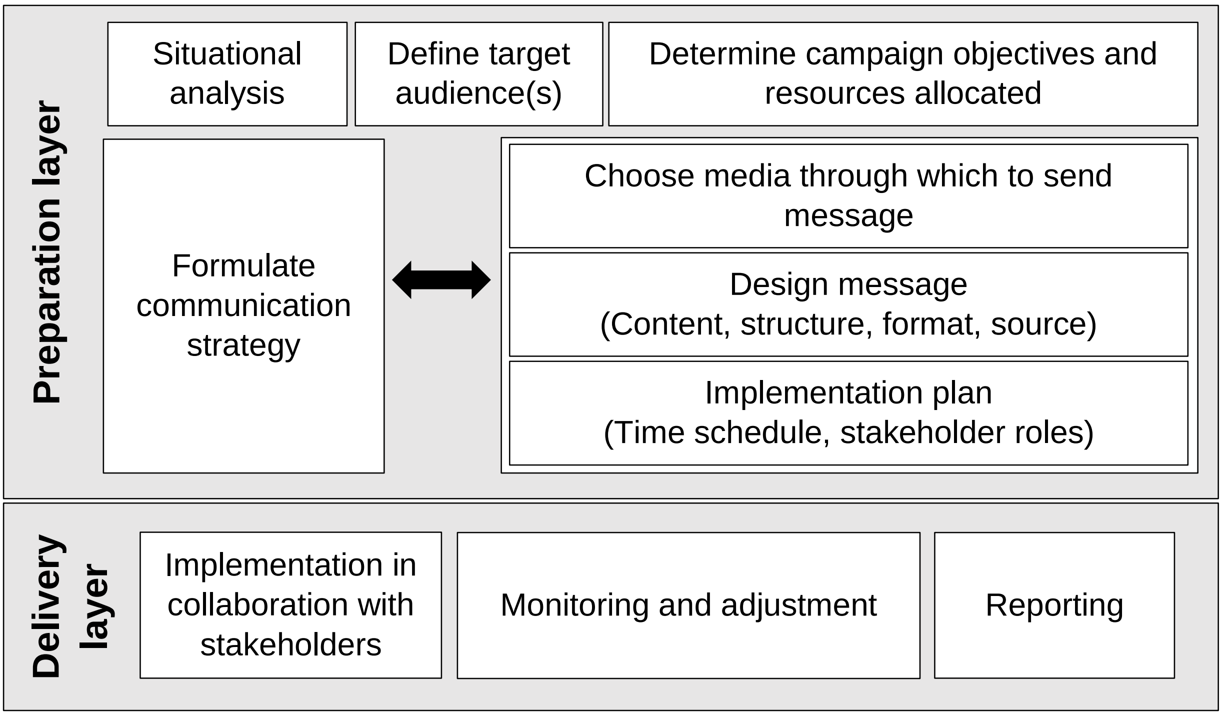

Preparation layer
Situational analysis
Define target audience(s)
Determine campaign objectives and resources allocated
Formulate communication strategy
Choose media through which to send message
Design message (Content, structure, format, source)
Implementation plan (Time schedule, stakeholder roles)
Delivery layer
Implementation in collaboration with stakeholders
Monitoring and adjustment
Reporting

Figure 14. Refined preparation and delivery layer

CHAPTER 5 SOUTH AFRICAN CYBER-SAFETY ACADEMIC ALLIANCE CAMPAIGN

“You might not change the past, but you might learn something from it.”

(Lewis Carroll, Alice's Adventures in Wonderland)

<table>
<tr><td colspan="3">**Entry vignette**
Abstract</td></tr>
<tr><td colspan="3">**Introduction to case and context**
Chapter one: Introduction
Research question:
What are the elements required for the preparation and delivery of a cyber-safety awareness campaign?</td></tr>
<tr><td colspan="3">Chapter two: Research methodology</td></tr>
<tr><td rowspan="3">**Research objective I.**
To identify, using existing literature, the essential elements required for conducting a cyber-safety awareness campaign in South Africa.</td><td colspan="2">**Description of case and context**</td></tr>
<tr><td>Chapter three:
Cyber-safety in South Africa</td><td>Chapter four:
Campaign planning</td></tr>
<tr><td>*Information Technology perspective*</td><td>*Communication Science perspective*</td></tr>
<tr><td>**Research objective II.**
To describe an existing South African cyber-safety awareness campaign aimed at schools, which forms the single case study;</td><td rowspan="2" colspan="2">**Development and detail about selected of issues**
Chapter five:
SACSAA campaign</td></tr>
<tr><td>**Research objective III.**
To compare the case study with the identified elements, and to determine whether there are any application gaps and areas for improvement;</td></tr>
<tr><td>**Research objective IV.**
To make recommendations for improved and integrated strategies for cyber awareness campaigns in South Africa.</td><td colspan="2">**Lessons learnt and closing vignette**
Chapter six:
Conclusion
Findings and recommendations</td></tr>
</table>

5.1 Introduction

The purpose of Chapter Five is to analyse the SACSAA cyber-security awareness campaign aimed at children, according to the preparation and delivery layers of the existing and proposed refined frameworks—as discussed in Chapter Four and Chapter Five. The analysis leads to an overview of the strengths and weaknesses of the current campaign, and identifies possible threats and opportunities for future campaigns.

5.2 South African Cyber-safety Academic Alliance (SACSAA)

Several Information Technology researchers from the Nelson Mandela Metropolitan University (NMMU), the University of Johannesburg (UJ) and the University of South Africa (UNISA) have been involved with C3 research. Cyber-security research at NMMU was conducted by the Institute of Information Communication Technology (IICTA), which was closed in 2013 to develop more focused research areas. In 2015, The NMMU Centre for Research in Information and Cyber-security (CRICS) was launched to focus on cyber-security research and related initiatives. Although CRICS is relatively new, research and initiatives for cyber-security awareness have been ongoing, ranging from awareness campaigns for children and university employees to workshops for teachers. Media coverage obtained by cyber-security researchers from the university include magazine (Vlok, 2014) and newspaper articles (Williams, 2014).

According to the UNISA website (http://eagle.unisa.ac.za/elmarie/), the Cyber-security Awareness project targets all age groups. Resources on the website, which range from a workbook, cyber pledge and posters, to research reports, point to the active involvement of UNISA in campaigns targeting children and the youth of South Africa. In contrast, UJ focus on industry and adult cyber-security needs through its Centre for Cyber-security, which operates in with the Academy of Computer Science and Software Engineering (University of Johannesburg, 2016).

Cyber-security researchers from the three universities established the South African Cyber-security Academic Alliance in 2011, to merge individual efforts and the existing material into a national cyber-safety initiative. SACSAA aims to inform all computer users in South Africa about cyber-security risks (Kortjan & Von Solms, 2014; Kritzinger & von Solms, 2012) through cyber-security campaigns.

Campaigns are short term initiatives (Evans-Lacko et al., 2010) developed to support a long-term integrated communication programme (Choo, 2011; Gregory, 2010).

SACSAA developed a two-part educational campaign for children. The first part of the campaign consists of educating children about cyber-safety risks through workbooks, school visits, posters, pamphlets and an annual awareness week. This is followed by a second part, which allows children to apply their knowledge through a poster contest (Van Niekerk, Thomson & Reid, 2013).

5.3 Existing framework

The current framework (Figure 15) considers topics, content, medium and tool selection during the preparation layer. The target audiences and roles as educator and learner are explored during the delivery layer.

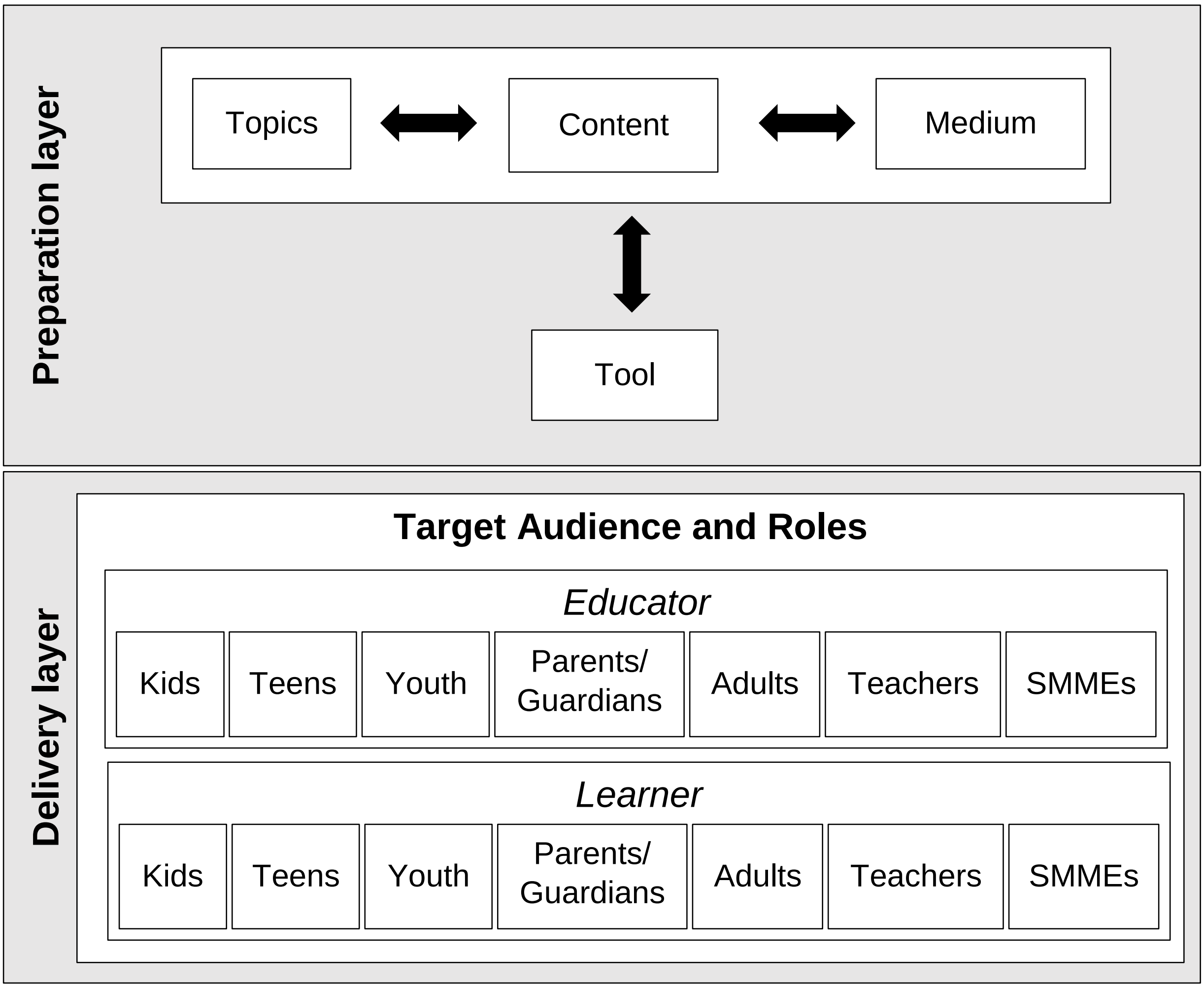


Figure 15. Existing framework layers

The existing framework layers are all implemented by SACSAA (Table 4). The alliance selected topics and content related to digital citizenship and C3 topics linked to cyber-ethics, cyber-security and cyber-safety. Medium and tool selection include the use of electronic and printed material, which is distributed through school visits and campaigns.

Table 4. Implementation of existing framework evident in SACSAA campaign material

Layer	Proposed activity during layer	Implemented by SACSAA
Preparation	Select topic, content and medium	Yes
	Select tool	Yes
Delivery	Select target audience and roles	Yes

5.4 Implementation of proposed refined framework

The manner in which the implementation of the application of the proposed refined layers to the SACSAA campaign is described in the following section. Various models and planning frameworks were discussed in Chapter Four to indicate the different stages required to develop effective campaigns, which led to proposed stages as outlined in Table 5.

Table 5. Planning stages for cyber-security campaign

Layer	Stage	Proposed activity during stage	Implemented by SACSAA
Preparation layer	**One**	Situational analysis	Yes
	Two	Define target audience	Partially
	Three	Determine campaign objectives and resources allocated	Partially
	Four	Formulate communication strategy • Media channel selection • Design message (content, structure, format, source) • Implementation plan (time schedule, stakeholder roles)	Partially
Delivery layer	**Five**	• Implement campaign in collaboration with stakeholders • Monitoring and adjustment • Reporting	Partially

The preparation layer includes the first four stages of the proposed stages and the fifth stage takes place in the delivery layer. The implementation of these stages as indicated by the right column in the table below, will be discussed in the following section.

5.5 Stage 1: Situational Analysis

At the start of campaign planning, it is important to conduct a situational analysis. The aim of the analysis is to have a clear purpose, strategic intent, scope and context in mind before planning any messages. SACSAA implemented the first planning stage.

SACSAA determined what the current cyber needs are and identified how the alliance can contribute towards creating a cyber-safe culture, through conducting a situational analysis supported by several research studies. Although schools are seen to be the key in securing a cyber-safe environment, SACSAA found that cyber-safety has not yet been incorporated into the South Africa school curriculum (South African Cyber-security Academic Alliance, 2016).

To address violence in schools, the National School Safety Framework (NSSF) was introduced to provide guidelines for school management and educators to deal effectively with safety concerns (Department of Basic Education, 2014). The framework lists cyberbullying as one of the incidents which could lead to violence in schools (Department of Basic Education, 2014), yet cyber-safety concerns are not addressed, even though school management and teachers have limited knowledge on cyber risks and how these risks should be dealt with when encountered by learners (Kritzinger, 2016). The Alliance recognises the present need for cyber-safety awareness and training for children (South African Cyber-security Academic Alliance, 2016). The purpose of the Alliance and the campaign has been established as contributing towards creating a cyber safe culture and filling a need for C3 awareness for children. The scope of the campaign has been limited to the South African context and, in particular, South African schools. It is not clear whether SACSAA conducted a SWOT analysis during the development of its campaigns.

5.6 Stage 2: Define target audience

The purpose of Stage Two is to define the target audience for the specific campaign. According to the SACSAA website (South African Cyber-security Academic Alliance, 2016), “cyber-security initiatives are aimed at school learners at the pre-primary, primary and secondary levels, students at tertiary level, industry, and interested parties from government, home users and anyone using the Internet".

Although these audiences are listed on the SACSAA website, it is not clear whether objectives have been set to reach each audience group. Campaign material is not targeted at a clearly defined target audience. Although SACSAA provides a list of the target audience, segmented according to demographic factors (age), existing campaign material that was developed for school children is target at several stakeholders.

If each audience group is not defined clearly according to their demographic and psychographic characteristics, the alliance may develop material which does not fulfil the intended outcome. School learners at pre-primary, primary and secondary levels, for instance, may require different materials to speak to their specific cyber needs, developed to communicate the message at the appropriate level.. Stage Two is therefore implemented only partially by SACSAA.

5.7 Stage 3: Determine campaign objectives and resources allocated

Once the context and target audience is clearly defined, Stage Three incorporates setting campaign objectives and determining the resources available. SACSAA states that their objective is "to campaign for the effective delivery of cyber-security awareness throughout South Africa to all population groups" (South African Cyber-security Academic Alliance, 2016). What has been labelled as an objective, can however, be seen as the mission of SACSAA. According to the SACSAA workbook, organising an annual cyber-security day in South Africa is seen as another short-term objective of the alliance (Kritzinger, 2012). However, organising an awareness day is an event or tool used to reach a set objective and not an objective in itself.

Setting SMARTA campaign objectives—objectives which are specific, measurable, attainable, relevant, time-bound and adjustable—for each campaign has not been implemented by SACSAA. SACSAA has considered the resources required to implement aspects of their awareness efforts and reported on the awareness and internalisation of information by children (Van Niekerk, Thomson & Reid, 2013), but results are measured based on objectives set at the start of a campaign. Stage Three was, therefore, only partially implemented as clear communication objectives were not visible for all campaigns.

5.8 Stage 4: Formulate communication strategy

The communication strategy for a campaign is developed in Stage Four. The stage includes media channel selection, message design and formulation of the implementation plan.

5.8.1 Media channel selection

Mediums and tools used by the alliance range from print to electronic resources. A primary school curriculum, SACSAA workbook, flyers and poster contest information are distributed to schools via mail and school visits, while the SACSAA website is also intended to act as a resource for users.

5.8.2 Message design

Message design aspects consider content, structure, format, and message source, which includes brand communication.

From the discussion in Chapter Three, it is clear that children grow up as digital citizens and need to be equipped with skills and knowledge to navigate themselves away from online risks while functioning in the cyber world. To equip children with the required knowledge and skills, SACSAA developed message content which address C3 topics. The inclusion of C3 topics in SACSAA material is summarised in Table 6.

Table 6. Evidence of C3 topics in SACSAA material

C3	Topic	SACSAA workbook	Cyber-safety 101 flyer	Facebook safety 101 flyer	Internet banking safety 101 flyer	Parental control 101 flyer	Public Wifi Safety 101 flyer
Cyberethics	Plagiarism	✓					
	Copyright	✓					
	Hacking	✓					
	Cyberbullying	✓					
	Copyright	✓	✓				
	Harassment	✓					
	Fair use	✓					
	File sharing	✓	✓				
	Online etiquette protocols	✓		✓			
	Posting incorrect/ inaccurate information	✓	✓	✓			

Table 6. Evidence of C3 topics in SACSAA material (continued)

C3	Topic	SACSAA workbook	Cyber-safety 101 flyer	Facebook safety 101 flyer	Internet banking safety 101 flyer	Parental control 101 flyer	Public Wifi Safety 101 flyer
	Stealing/pirating software, music and video	✓	✓			✓	
	Online gambling	✓					
	Gaming	✓					
	Internet addiction	✓					
Cybersafety	Online predators	✓					
	Objectionable content	✓					
	Cyberstalking	✓					
	Downloading	✓				✓	
	Paedophiles	✓					
	Hate groups	✓					
	Pornography	✓					
	Unwanted communication	✓					
	Online threats	✓		✓		✓	
Cyber-security	Hoaxes	✓	✓		✓		
	Viruses and other malicious self-replicating code	✓	✓	✓	✓		✓
	Junk e-mail	✓		✓	✓		
	Chain letters	✓		✓	✓		
	Ponzi schemes	✓		✓	✓		
	Get-rich-quick schemes	✓	✓	✓	✓		
	Scams	✓	✓	✓	✓		
	Criminal hackers	✓		✓	✓		✓
	Hacktivists	✓		✓	✓		
	Spyware	✓		✓	✓		✓
	Adware	✓		✓	✓		
	Malware	✓	✓	✓	✓		✓
	Trojans	✓	✓				
	Phishing	✓	✓				
	Pharming scams	✓					
	Theft of identity	✓	✓				
	Spoofing	✓					
	Privacy	✓	✓				

Table 6. Evidence of C3 topics in SACSAA material (continued)

Topic	SACSAA workbook	Cyber-safety 101 flyer	Facebook safety 101 flyer	Internet banking safety 101 flyer	Parental control 101 flyer	Public Wifi Safety 101 flyer
Other				Passwords Privacy settings Online reputation	Parental control software Restrictions User accounts	Information encryption Firewalls

The topics and content are structured and formatted by SACSAA. Message structure, format and source includes iconic, symbolic, or indexical images or a combination of visuals (Epure, Eisenstat & Dinu, 2014; Grbich, 2013). Iconic images refer to a visual element representing an actual object (Grbich 2013) as, for example in a picture of a laptop. Symbolic images relate to a visual element with a learnt association (Grbich 2013)—for example, a lock displayed with a computer, associated with information security. Indexical images refer to the meaning of visual elements in a particular context, category or natural event (Grbich 2013), as in, for example, the use of a finger pointing to information to highlight its importance in cyber-safety material.

SACSAA introduced a mascot, called Cyber Safe Robot, as part of the SACSAA workbook. The mascot concept was developed further and now includes Cyber Sid and Cyber Sindy (Figure 16).

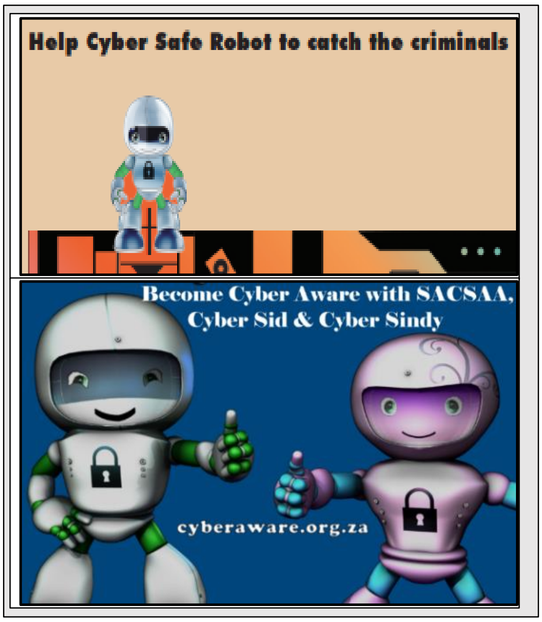

Help Cyber Safe Robot to catch the criminals
Become Cyber Aware with SACSAA,
Cyber Sid & Cyber Sindy
cyberaware.org.za

Figure 16. SACSAA Mascots

Mascots contribute towards message source credibility and can have the same influence as celebrities (Pairoa & Arunrangsiwed, 2016). In America, well-known personalities, such as Hillary Clinton (Hughes, 2016) and Michelle Obama (Sheperd, 2011) voiced their support for initiatives to protect children against threats online. The same level of endorsements from South African celebrities has not yet been secured by SACSAA, but the potential for collaboration exists once the SACSAA brand and mascots are more established. Although teachers have indicated that the robot may not apply to children and that stock images of learners taking 'selfies' would be more applicable, the robot was included extensively by children in the 2014 poster contest, as indicated by a selection of the poster examples (Figure 17).

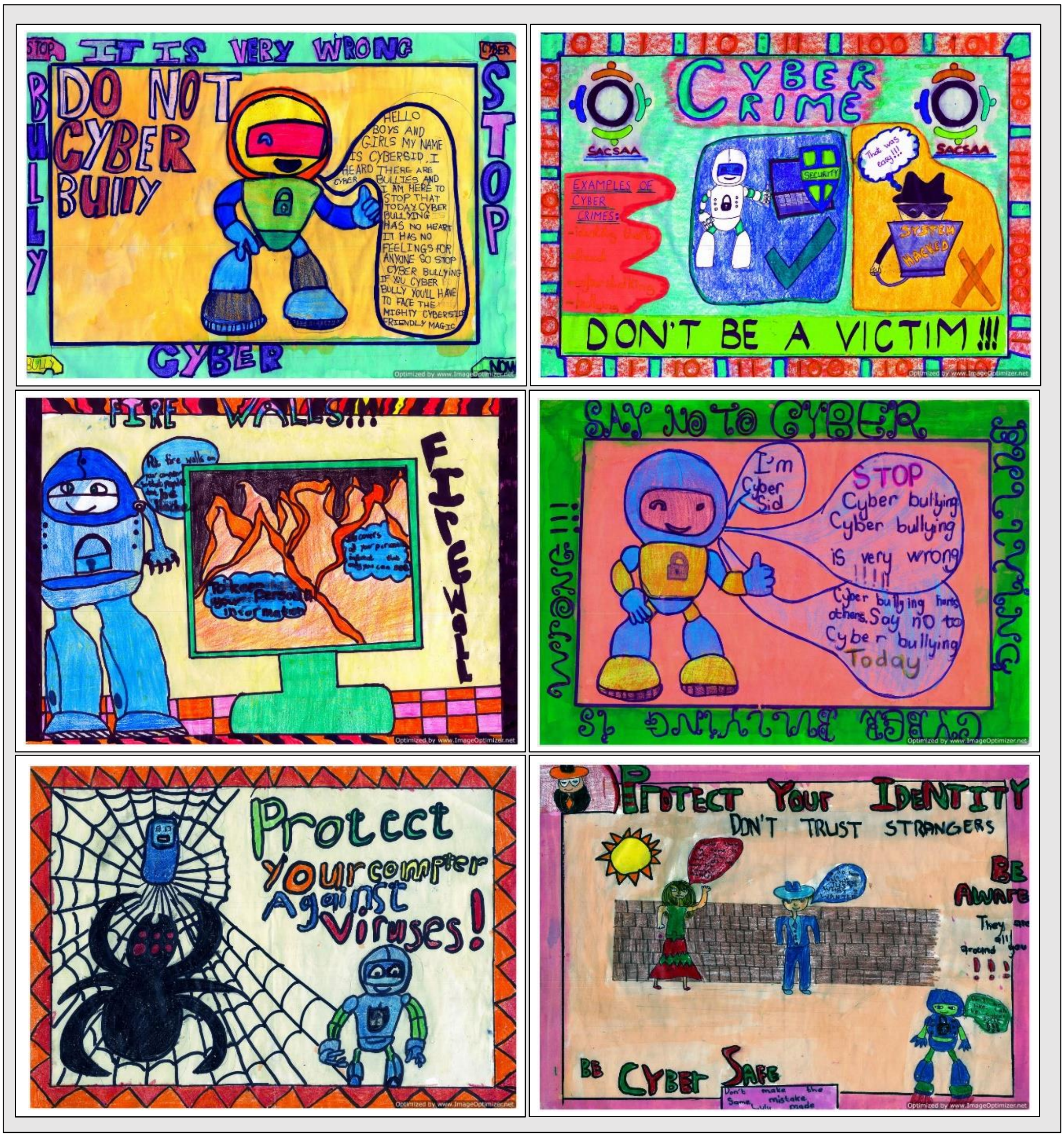

STOP
IT IS VERY WRONG
CYBER
BULLY
DO NOT CYBER BULLY
STOP
HELLO BOYS AND GIRLS MY NAME IS CYBERSID. I HEARD THERE ARE CYBER BULLIES AND I AM HERE TO STOP THAT TODAY. CYBER BULLYING HAS NO HEART IT HAS NO FEELINGS FOR ANYONE SO STOP CYBER BULLYING IF YOU CYBER BULLY YOU'LL HAVE TO FACE THE MIGHTY CYBERSID FRIENDLY MAGIC
CYBER
BULLY
NOW
0 1 10 11 100 101
CYBER CRIME
SACSAA
SACSAA
EXAMPLES OF CYBER CRIMES:
SECURITY
That was easy!!!
SYSTEM HACKED
DON'T BE A VICTIM !!!
FIRE WALLS!!!
FIREWALL
To keep your personal information
SAY NO TO CYBER BULLYING IS WRONG!!!
I'm Cyber Sid
STOP Cyber bullying Cyber bullying is very wrong !!!!!
Cyber bullying hurts others. Say no to Cyber bullying Today
Protect your compter Against Viruses!
PROTECT YOUR IDENTITY
DON'T TRUST STRANGERS
BE AWARE
They are all around you !!!
BE CYBER SAFE
Don't make the same mistake Lulu made

Figure 17. Use of SACSAA mascot in poster designs

Individual university branding guidelines are currently used, and the SACSAA logo, website address or mascot are added to these materials. The SACSAA website does not contain a document explaining the development and significance of the logo used for the alliance, but it is clear that the logo includes an annular element surrounded by four icons (Figure 18).

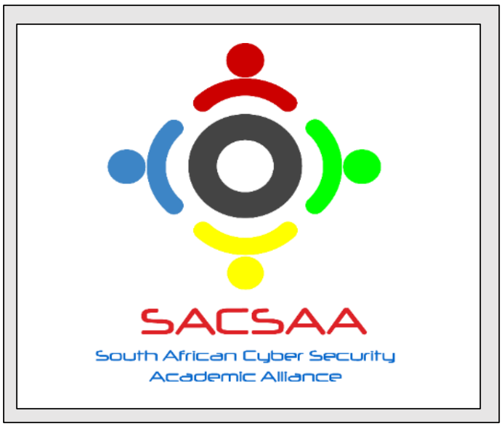


Figure 18. SACSAA logo

The annular element of the logo is the only similarity in design with the NMMU logo, while the placement of text below the logo, and is the only similarity in design with the UJ logo (Figure 19).

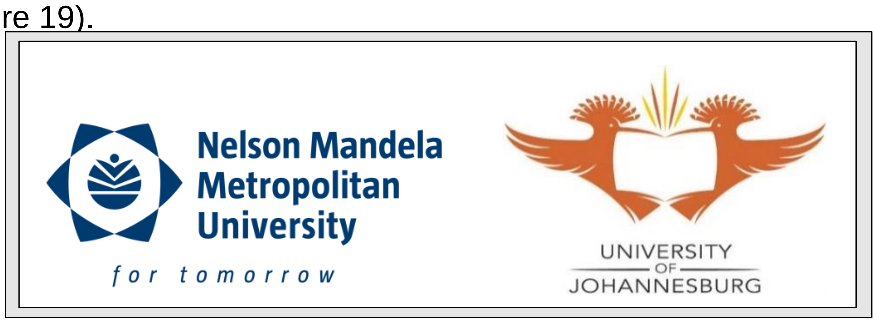
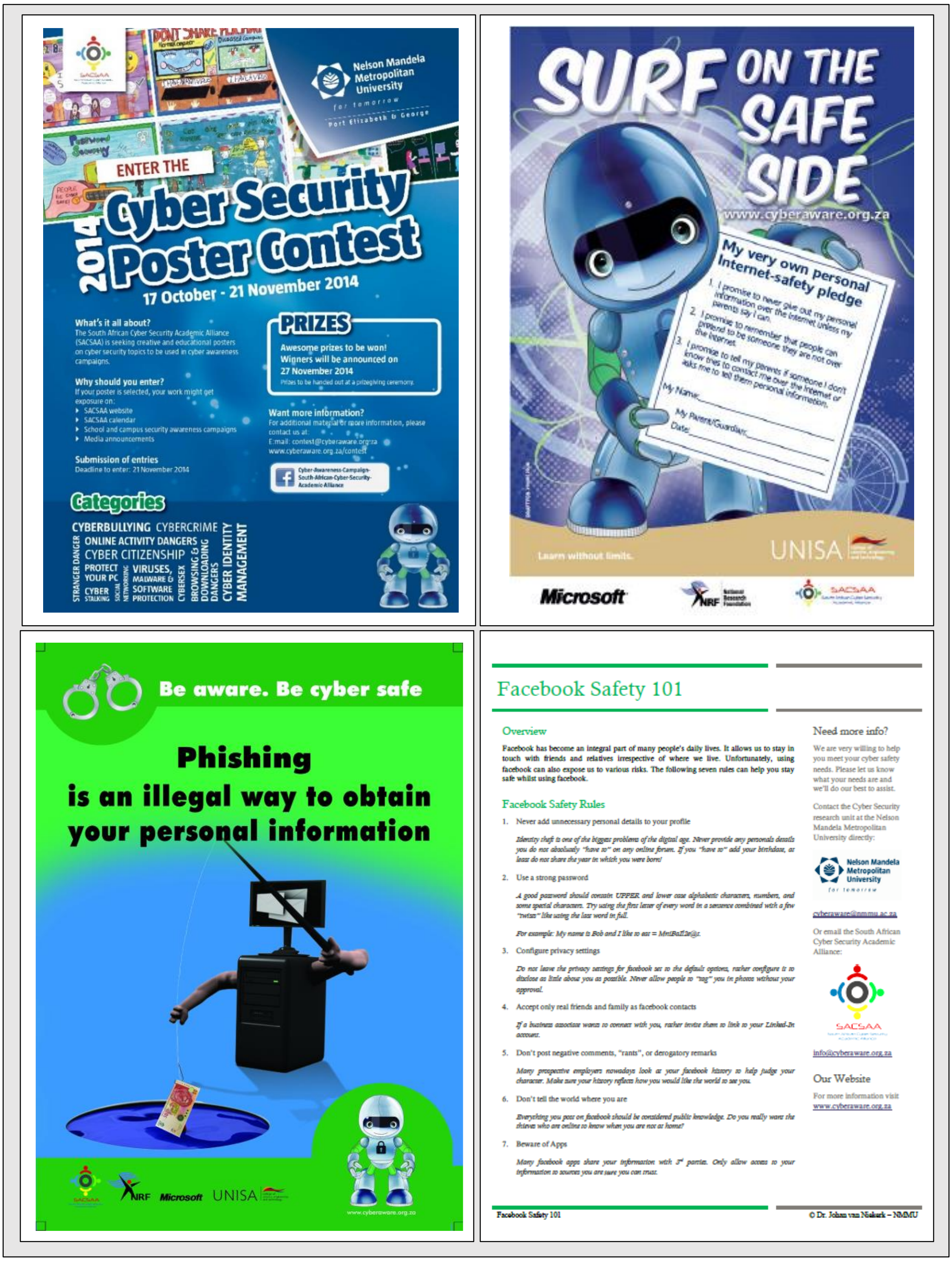


Figure 19. NMMU and UJ logo

The inclusion of the annular element in the NMMU logo points to continuous development and innovation (NMMU, 2016), which can also be applied to the SACSAA logo. The four icons surrounding the circle, represents humans working together to develop and innovate new cyber-safety and security initiatives. De Bono developed the six thinking hat system which links colour to different types of thinking and can be applied to meeting settings or teamwork (Gregory & Masters, 2012; Rao, 2015; Vernon & Hocking, 2014). The four colours used in the SACSAA logo for the human icons are red, blue, green and yellow. According to De Bono, red considers emotions or feelings; blue thinking represents control and the thinking involved in finding solutions to problems (Kivunja, 2015). Green represents creative thinking, and yellow represents constructive, positive thinking (Liu, Zehtabchi & Liteplo, 2014; Pinto, Barreto, Praça, Sousa, Vale & Solteiro Pires, 2015).

Clear brand guidelines cannot be identified from existing material as logo use and placement, the inclusion of the mascot, and general designs employed by the Alliance are not similar. Figure 20 provides examples to illustrate the different approaches used.



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

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

Cyber-Awareness-Campaign-South-African-Cyber-Security-Academic-Alliance

My very own personal Internet-safety pledge

1. I promise to never give out my personal information over the Internet unless my parents say I can.
2. I promise to remember that people can pretend to be someone they are not over the Internet.
3. I promise to tell my parents if someone I don't know tries to contact me over the Internet or asks me to tell them personal information.

My Name:__________

My Parent/Guardian:__________

Date:__________

Facebook Safety 101

Overview

Facebook has become an integral part of many people's daily lives. It allows us to stay in touch with friends and relatives irrespective of where we live. Unfortunately, using facebook can also expose us to various risks. The following seven rules can help you stay safe whilst using facebook.

Facebook Safety Rules

1. Never add unnecessary personal details to your profile

   Identity theft is one of the biggest problems of the digital age. Never provide any personals details you do not absolutely "have to" on any online forum. If you "have to" add your birthdate, at least do not share the year in which you were born!

2. Use a strong 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 = MniBaIl2e@t.

3. Configure privacy settings

   Do not leave the privacy settings for facebook set to the default options, rather configure it to disclose as little about you as possible. Never allow people to "tag" you in photos without your approval.

4. Accept only real friends and family as facebook contacts

   If a business associate wants to connect with you, rather invite them to link to your Linked-In account.

5. Don't post negative comments, "rants", or derogatory remarks

   Many prospective employers nowadays look at your facebook history to help judge your character. Make sure your history reflects how you would like the world to see you.

6. Don't tell the world where you are

   Everything you post on facebook should be considered public knowledge. Do you really want the thieves who are online to know when you are not at home?

7. Beware of Apps

   Many facebook apps share your information with 3rd parties. Only allow access to your information to sources you are sure you can trust.

Need more info?

We are very willing to help you meet your cyber safety needs. Please let us know what your needs are and we'll do our best to assist.

Contact the Cyber Security research unit at the Nelson Mandela Metropolitan University directly:

Nelson Mandela Metropolitan University for tomorrow

cyberaware@nmmu.ac.za

Or email the South African Cyber Security Academic Alliance:

SACSAA

info@cyberaware.org.za

Our Website

For more information visit www.cyberaware.org.za

Facebook Safety 101 © Dr. Johan van Niekerk – NMMU

Figure 20. Sample campaign material from SACSAA

A combination of iconic and symbolic images (Grbich, 2013) are used on the SACSAA website (Figure 21). Iconic images include photographs taken at SACSAA school visits or workshops, a photo of the SACSAA school curriculum material, and a copy of a newspaper article. These pictures represent the work done by the Alliance.

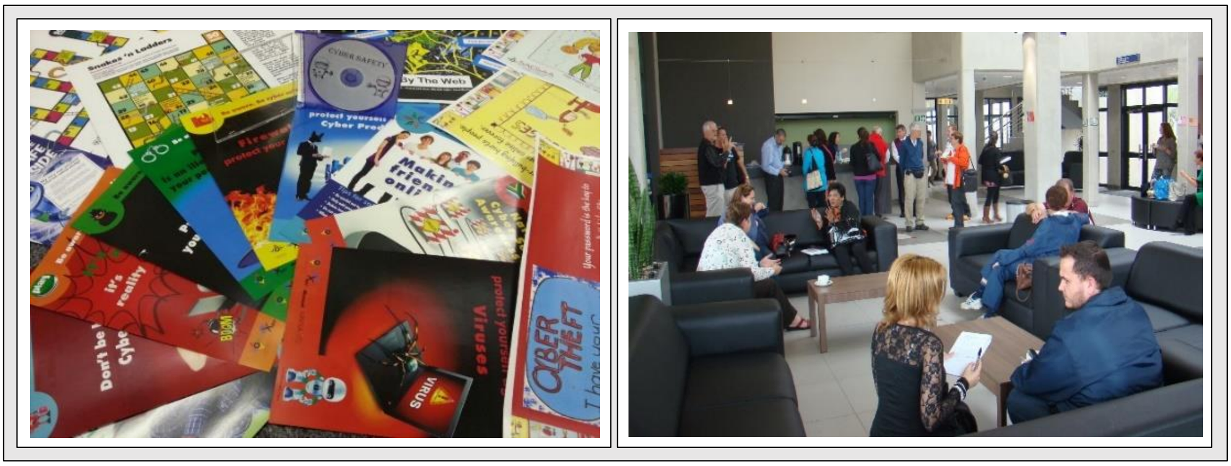


Figure 21. Iconic images used by SACSAA

Cyber Sid and Cyber Sindy serve as symbolic images which represents the alliance and what the purpose of the alliance is. The mascots are associated with cyber-safety include the use of SACSAA mascots (Figure 22).

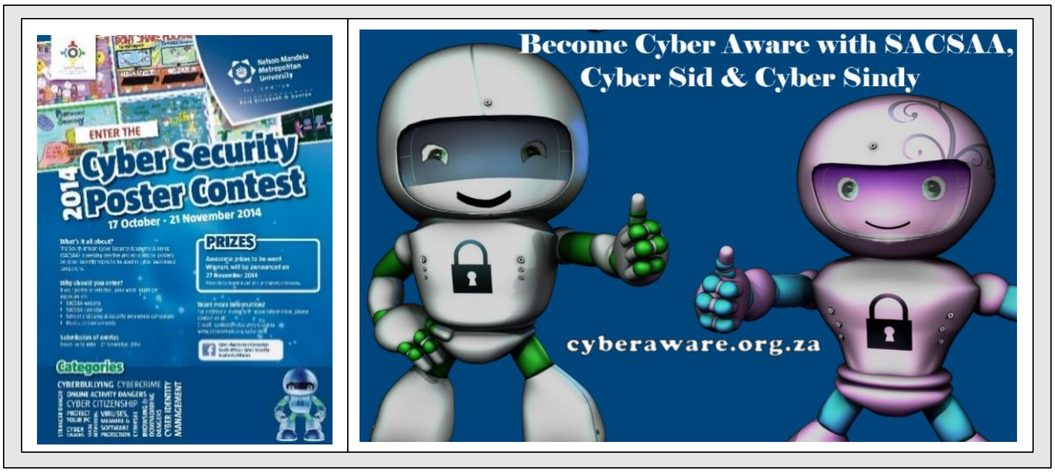
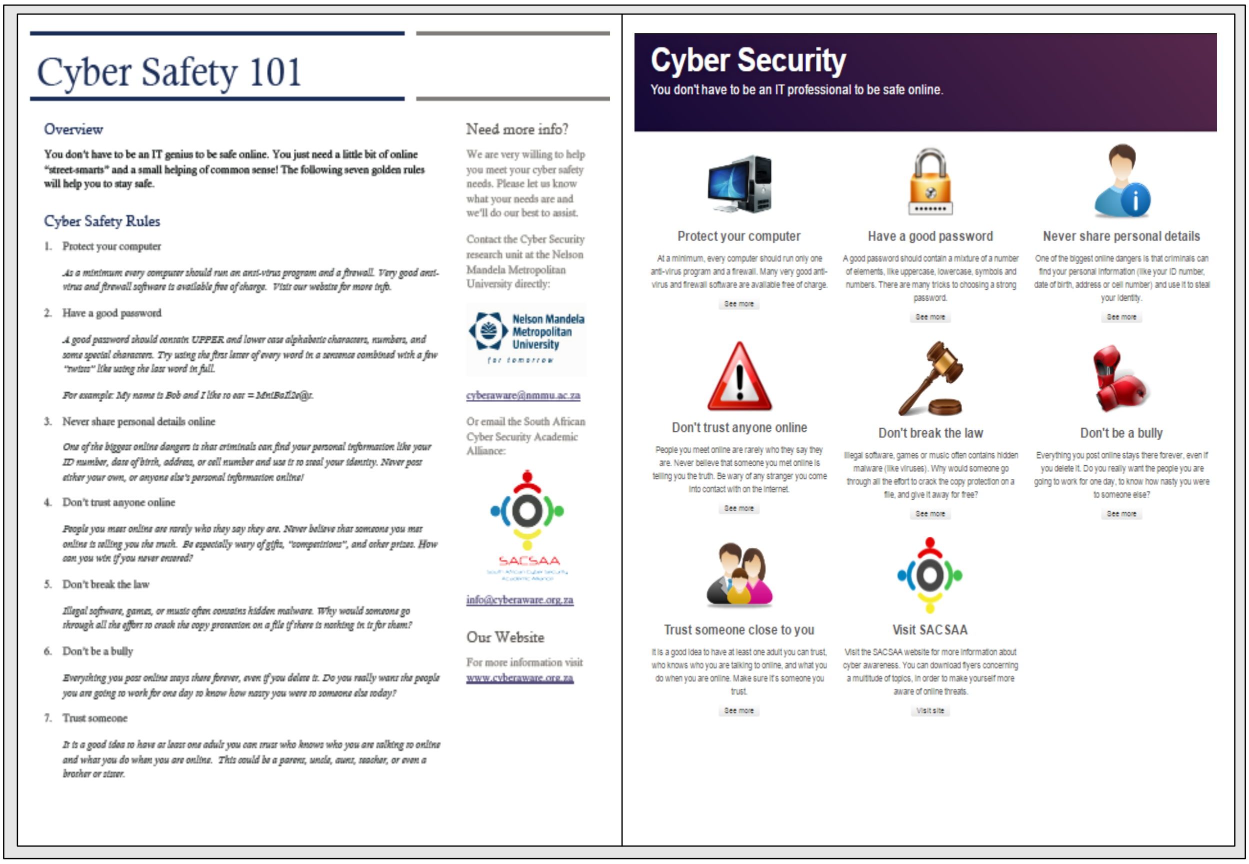

ENTER THE
2014 Cyber Security Poster Contest
17 October - 21 November 2014
PRIZES
Categories
Become Cyber Aware with SACSAA,
Cyber Sid & Cyber Sindy
cyberaware.org.za

Figure 22. Symbolic images used on website

The use of visual elements in campaign material is essential to attract the attention of the target audience. The flyer developed serves as an example of information presented without visual elements, compared to the presentation of the same material on the

SACSAA website, with images (Figure 23). The figure on the right hand side is more visually appealing due to the inclusion of images and several colours.



Cyber Safety 101

Overview

You don't have to be an IT genius to be safe online. You just need a little bit of online "street-smarts" and a small helping of common sense! The following seven golden rules will help you to stay safe.

Cyber Safety Rules

1. Protect your computer

   As a minimum every computer should run an anti-virus program and a firewall. Very good anti-virus 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 = MniBaIl2e@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. Don't 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. Don't 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.

Need more info?

We are very willing to help you meet your cyber safety needs. Please let us know what your needs are and we'll do our best to assist.

Contact the Cyber Security research unit at the Nelson Mandela Metropolitan University directly:

cyberaware@nmmu.ac.za

Or email the South African Cyber Security Academic Alliance:

info@cyberaware.org.za

Our Website

For more information visit www.cyberaware.org.za

Cyber Security

You don't have to be an IT professional to be safe online.

Protect your computer

At a minimum, every computer should run only one anti-virus program and a firewall. Many very good anti-virus and firewall software are available free of charge.

Have a good password

A good password should contain a mixture of a number of elements, like uppercase, lowercase, symbols and numbers. There are many tricks to choosing a strong password.

Never share personal details

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.

Don't 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 wary of any stranger you come into contact with on the internet.

Don't break the law

Illegal software, games or music often contains hidden malware (like viruses). Why would someone go through all the effort to crack the copy protection on a file, and give it away for free?

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?

Trust someone close to you

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. Make sure it's someone you trust.

Visit SACSAA

Visit the SACSAA website for more information about cyber awareness. You can download flyers concerning a multitude of topics, in order to make yourself more aware of online threats.

Figure 23. Cyber-safety 101 information with and without visual elements

5.8.3 Implementation plan

There is no clear timeline for SACSAA initiatives as the Alliance website is outdated; as can be seen with broken links, and references to information which was not published on the website in 2014 and 2015. There is no reference to the 2016 poster contest and new campaign material is not made available on the site. Although visitors to the SACSAA website cannot access financial information, the development of SACSAA material and the poster contest indicates that the Alliance has funding available to implement campaigns. Based on the outdated online platforms, it appears as though the alliance may not have enough human resources for online content management.

Taking into consideration the media channel selection, message design and implementation plan, Stage Four was partially implemented by SACSAA. Some communication channels are used to communicate with the intended audience and some of the materials, such as the workbook adhere to visually appealing design principles through the use of colour and design.

5.9 Stage 5: Implementing, monitoring and reporting on campaign

It is unclear whether SACSAA views individual efforts by UNISA, UJ and NMMU as separate campaigns which link to the overall mission of creating a safe cyber culture in South Africa, or whether all initiatives are viewed as one cyber-safety campaign for the Alliance. The implementation tactics focuses on the internal and external conditions which affect the efforts of SACSAA. Examples include incorporating different ways to reach the target audience and considering social considerations, such as languages spoken by the target audience. The SACSAA booklet was translated and is available in Afrikaans, English, Tswana and IsiZulu. It is not clear whether school-specific or city-specific considerations have been used when compiling materials.

Since the inception of the Alliance, SACSAA has developed a website to provide access to these resources; and it is continuously working on those activities which will educate Internet users on the cyber risks. The website is discussed in order of the site tabs indicated below (Figure 24).

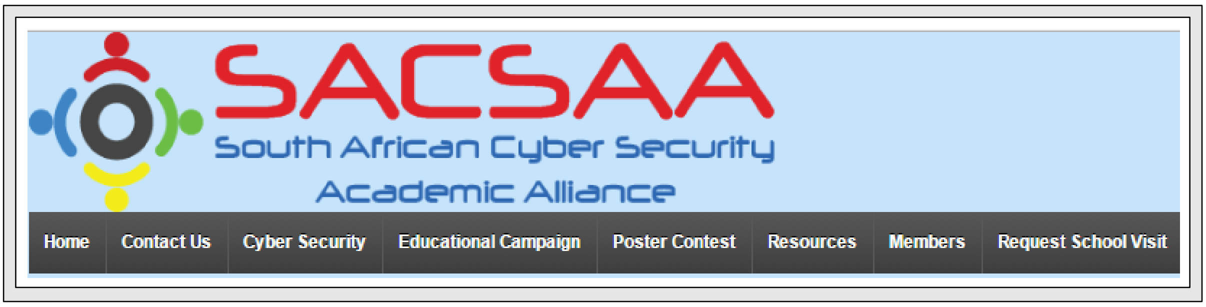
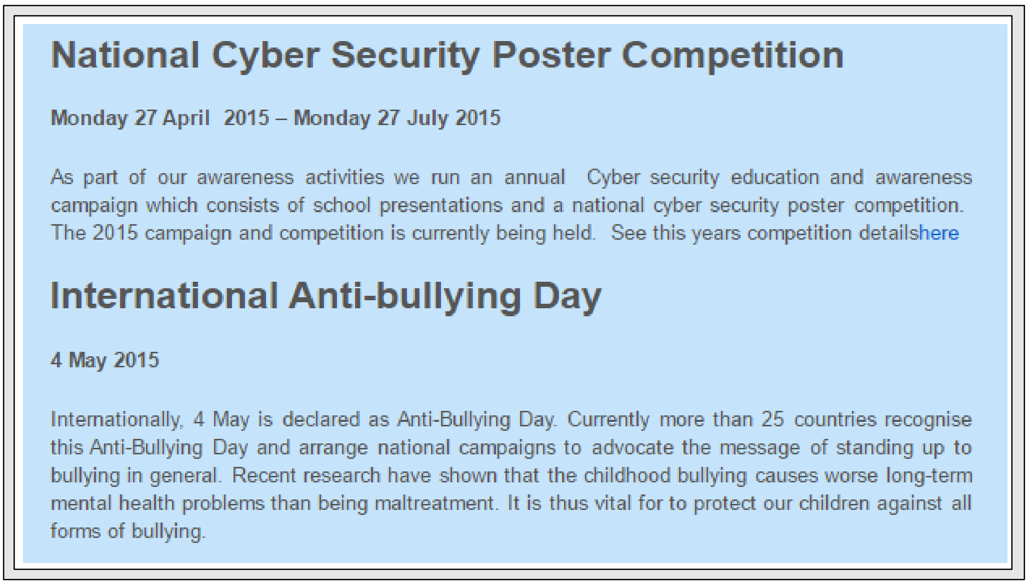


Figure 24. SACSAA website

5.9.1 Homepage tab

The home tab of the SACSAA website welcomes users to the SACSAA site, provides an overview of the purpose of the Alliance and explains how cyber-security awareness can be gained as a life skill. As indicated in Figure 25, the home page also includes information about the 2015 national cyber-security poster competition, 2015 international Anti-bulling Day, and an indication that more details will be provided later regarding a national cyber-security awareness week. The home page does not refer to the 2016 dates for these events.



National Cyber Security Poster Competition

Monday 27 April 2015 – Monday 27 July 2015

As part of our awareness activities we run an annual Cyber security education and awareness campaign which consists of school presentations and a national cyber security poster competition. The 2015 campaign and competition is currently being held. See this years competition detailshere

International Anti-bullying Day

4 May 2015

Internationally, 4 May is declared as Anti-Bullying Day. Currently more than 25 countries recognise this Anti-Bullying Day and arrange national campaigns to advocate the message of standing up to bullying in general. Recent research have shown that the childhood bullying causes worse long-term mental health problems than being maltreatment. It is thus vital for to protect our children against all forms of bullying.

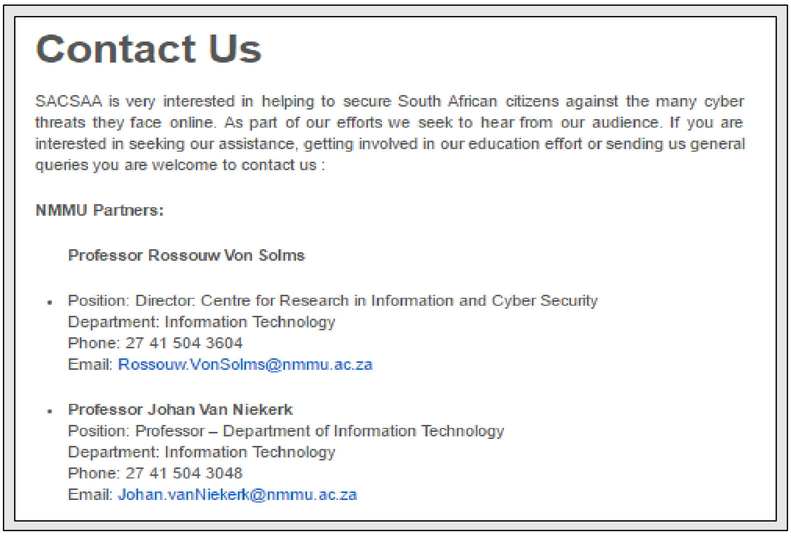
Figure 25. SACSAA home page

The home page also contains an icon for a South African radio station, RSG (Figure 26). The icon does not link to any content or the RSG website. There are no references made to the radio station on the website.

Figure 26. RSG icon

5.9.2 Contact us

This section invites the user to submit questions to the NMMU partners of SACSAA (Figure 27). No mention is made of UJ, UNISA or other members of NMMU involved with SACSAA.



Contact Us

SACSAA is very interested in helping to secure South African citizens against the many cyber threats they face online. As part of our efforts we seek to hear from our audience. If you are interested in seeking our assistance, getting involved in our education effort or sending us general queries you are welcome to contact us :

NMMU Partners:

Professor Rossouw Von Solms

- Position: Director: Centre for Research in Information and Cyber Security
  Department: Information Technology
  Phone: 27 41 504 3604
  Email: Rossouw.VonSolms@nmmu.ac.za

- Professor Johan Van Niekerk
  Position: Professor – Department of Information Technology
  Department: Information Technology
  Phone: 27 41 504 3048
  Email: Johan.vanNiekerk@nmmu.ac.za

Figure 27. Contact Us

5.9.3 Cyber-security tab

The cyber-security tab further extends to general information, cyber-safety curriculum for primary schools, cyber-security rules, and cyber-security 101 flyers (Figure 28).

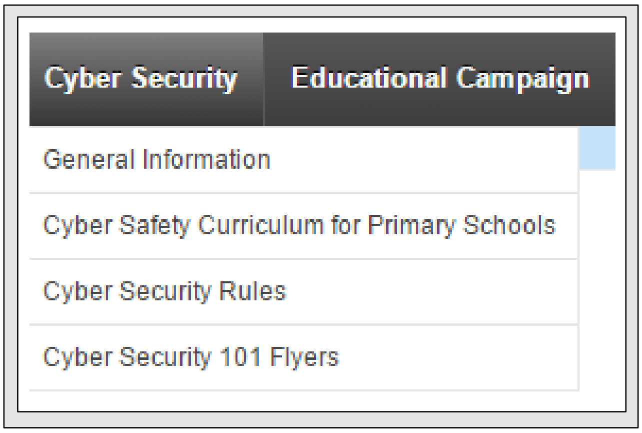
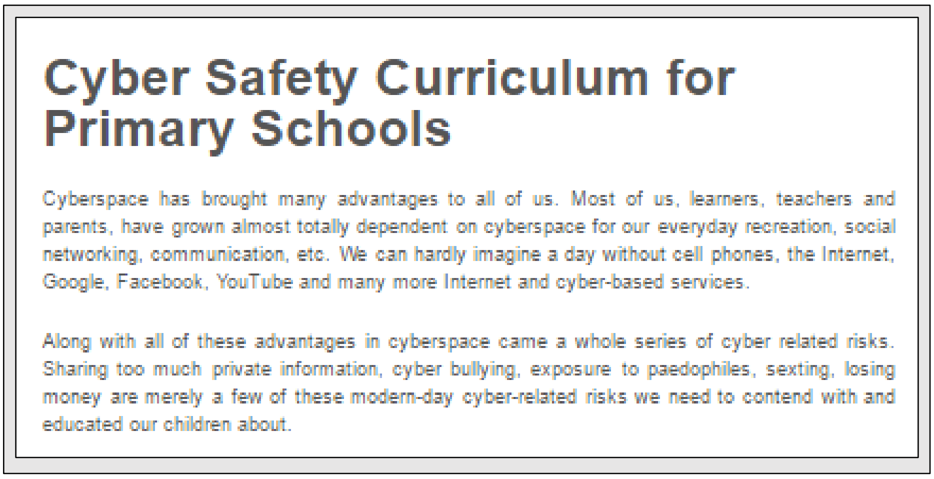


Figure 28. Cyber-security tab

The general information section provides an overview of what cyber-security entails and why it is important to be aware of cyber risks. The following topics are also briefly discussed: malware, cyberbullying, social networking, identity theft, phishing.



Cyber Safety Curriculum for Primary Schools

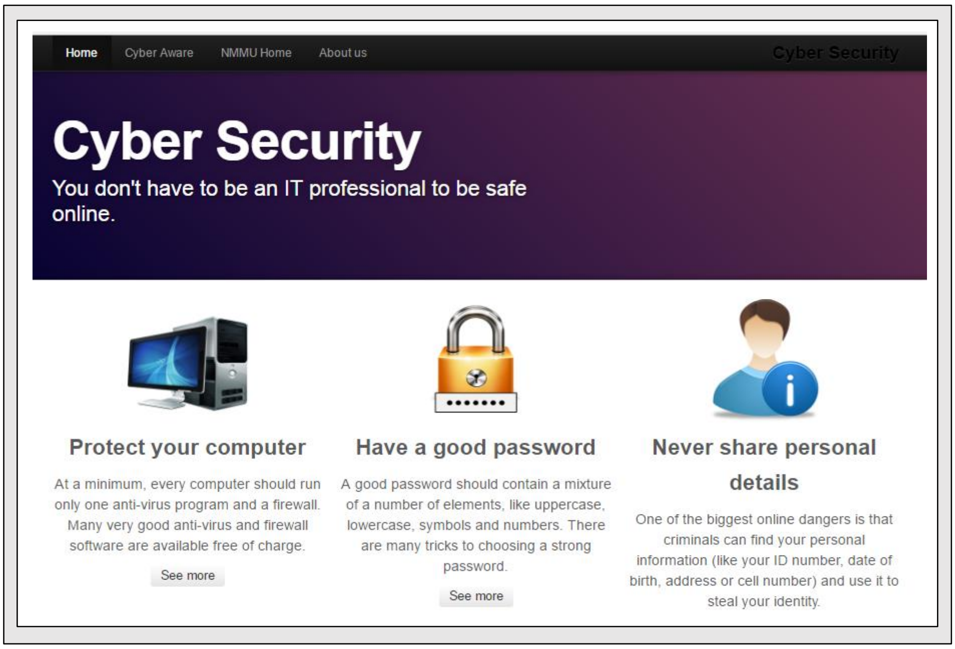
Cyberspace has brought many advantages to all of us. Most of us, learners, teachers and parents, have grown almost totally dependent on cyberspace for our everyday recreation, social networking, communication, etc. We can hardly imagine a day without cell phones, the Internet, Google, Facebook, YouTube and many more Internet and cyber-based services.

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 educated our children about.

Figure 29. Cyber-safety Curriculum for Schools

The Alliance found that not all teachers have the knowledge required to teach children about cyber-safety and have access to resources, which would assist them in understanding the risks involved with cyber use. In response to this challenge, SACSAA developed a cyber-safety curriculum (Figure 29) and introduced it to teachers in the Nelson Mandela Bay Metropole in 2014. The curriculum is available to primary schools at no cost. The cyber-safety curriculum for primary schools section explains the purpose of the curriculum and invites primary school teachers to request the free material by filling out their details on the website.

The cyber-security rules tab links to a section of the website which uses a different format and design style to the rest of the site (Figure 30). Images are accompanied with short snippets of information about good practices.



Cyber Security

You don't have to be an IT professional to be safe online.

Protect your computer

At a minimum, every computer should run only one anti-virus program and a firewall. Many very good anti-virus and firewall software are available free of charge.

Have a good password

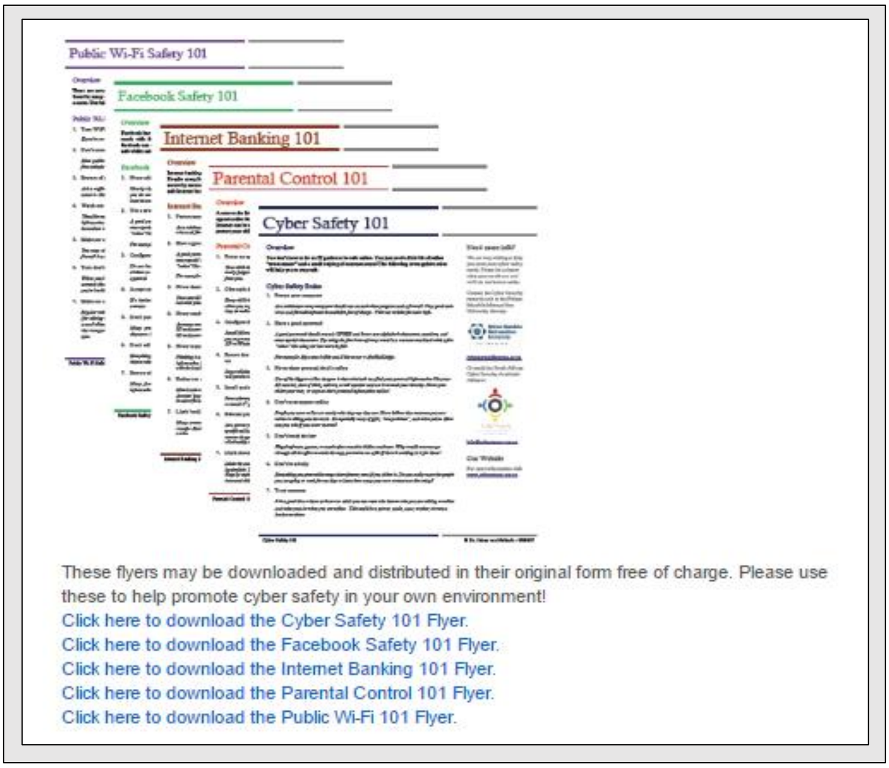
A good password should contain a mixture of a number of elements, like uppercase, lowercase, symbols and numbers. There are many tricks to choosing a strong password.

Never share personal details

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.

Figure 30. Cyber-security rules

The cyber-security 101 flyers (Figure 31) are available for download and address the following topics: Facebook safety 101, cyber-security 101, parental control 101, public Wi-Fi 101 and Internet banking 101.



These flyers may be downloaded and distributed in their original form free of charge. Please use these to help promote cyber safety in your own environment!
Click here to download the Cyber Safety 101 Flyer.
Click here to download the Facebook Safety 101 Flyer.
Click here to download the Internet Banking 101 Flyer.
Click here to download the Parental Control 101 Flyer.
Click here to download the Public Wi-Fi 101 Flyer.

Figure 31. SACSAA flyers

5.9.4 Educational campaign

The Educational Campaign tab provides information about the SACSAA school campaign and awareness week (Figure 32).

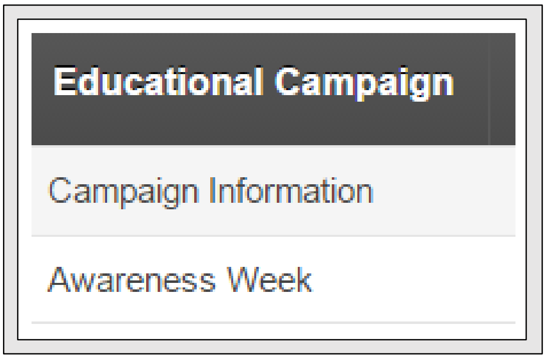


Figure 32. Educational campaign

5.9.5 Poster contest tab

The poster contest tab includes information about the current competition, provides examples of past competition entries and competition guidelines from 2011 to 2015, as well as a section for visitors to request poster competition flyers for schools (Figure 33).

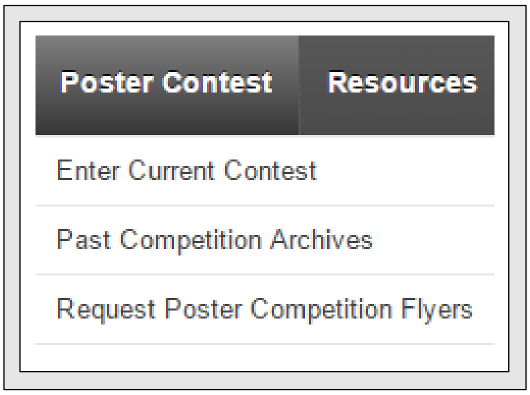
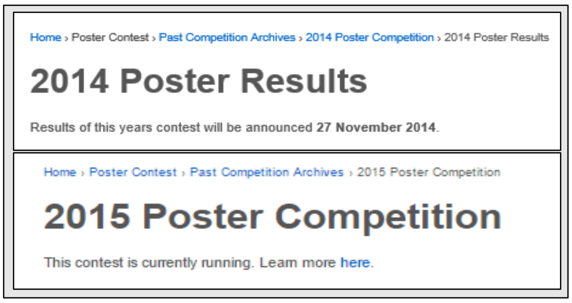


Figure 33. Poster contest

The entry requirements, including contestant guidelines, poster guidelines, content guidelines and how to submit posters for 2015 are discussed in the current contest section (Figure 34). The 2016 competition information is not available on the website.



Home › Poster Contest › Past Competition Archives › 2014 Poster Competition › 2014 Poster Results

2014 Poster Results

Results of this years contest will be announced **27 November 2014**.

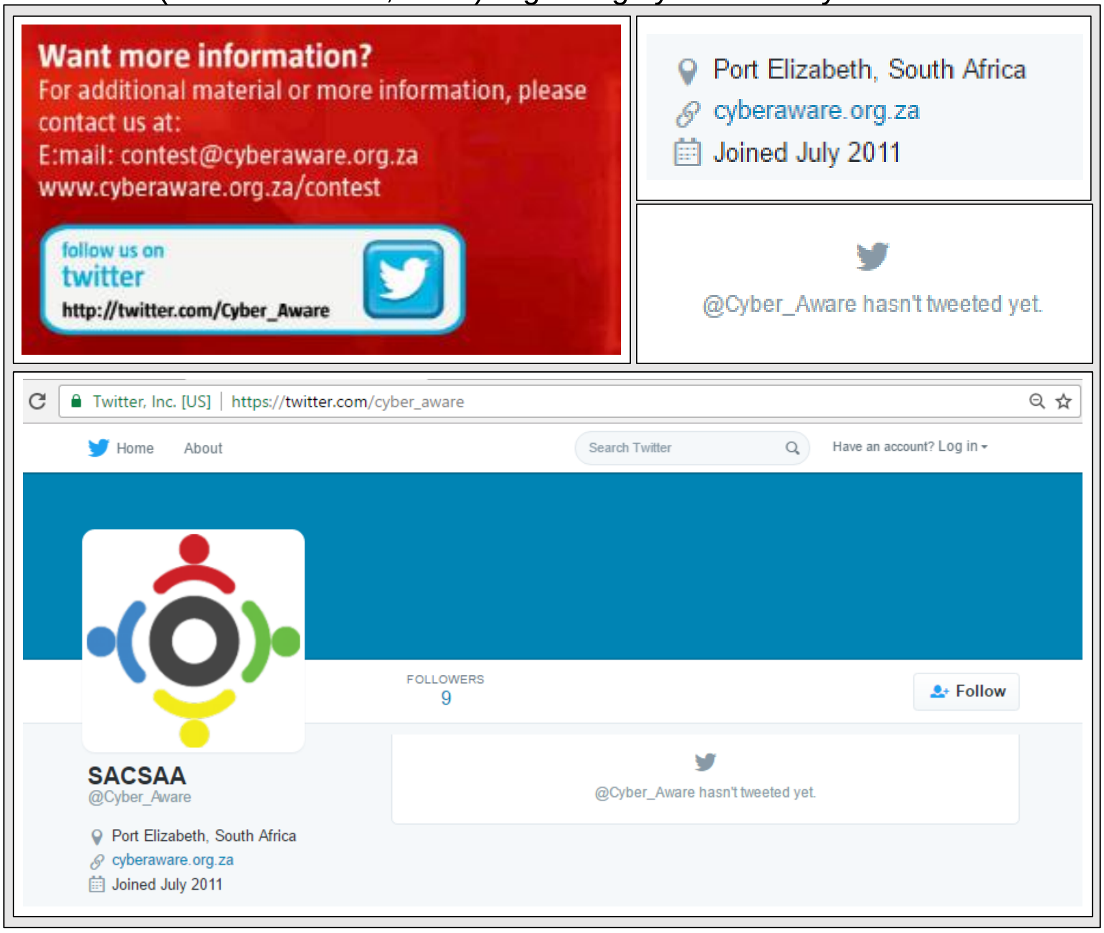
Home › Poster Contest › Past Competition Archives › 2015 Poster Competition

2015 Poster Competition

This contest is currently running. Learn more here.

Figure 34. Poster competition information

The poster competition flyers refer to the Twitter account of SACSAA (Figure 35), but the site contains no tweets. Social media tools create the opportunity to facilitate conversations (Fraustino & Ma, 2015) regarding cyber-security issues.



Want more information?
For additional material or more information, please contact us at:
E:mail: contest@cyberaware.org.za
www.cyberaware.org.za/contest

follow us on twitter
http://twitter.com/Cyber_Aware

Port Elizabeth, South Africa
cyberaware.org.za
Joined July 2011

@Cyber_Aware hasn't tweeted yet.

Twitter, Inc. [US] | https://twitter.com/cyber_aware

FOLLOWERS
9

SACSAA
@Cyber_Aware

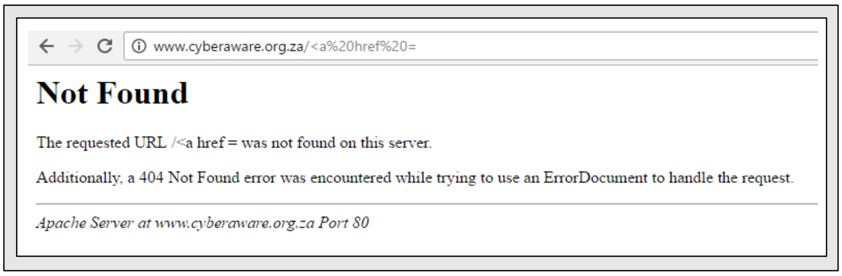
@Cyber_Aware hasn't tweeted yet.

Port Elizabeth, South Africa
cyberaware.org.za
Joined July 2011

Figure 35. SACSAA Twitter account

5.9.6 Resources tab

The external resources link to additional material on the UNISA website. The link, however, directs users to an inactive site (Figure 36).



www.cyberaware.org.za/<a%20href%20=

Not Found

The requested URL /<a href = was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

Apache Server at www.cyberaware.org.za Port 80

Figure 36. Inactive UNISA link

The tab also directs users to complete an online form to join SACSAA or to link to the UJ website to report cybercrime (Figure 37).

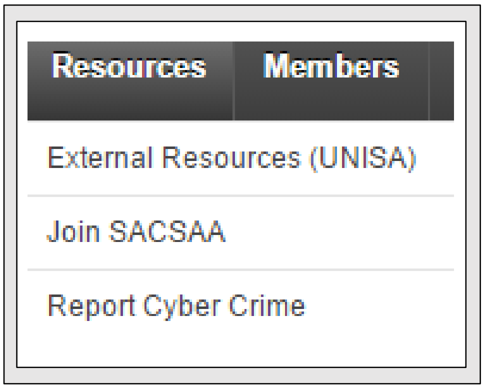


Figure 37. Resources tab

5.9.7 Members tab

The member's tab provides links to the individual websites of the three founding universities (Figure 38).

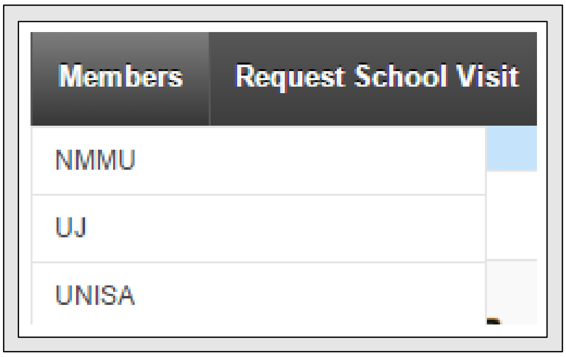
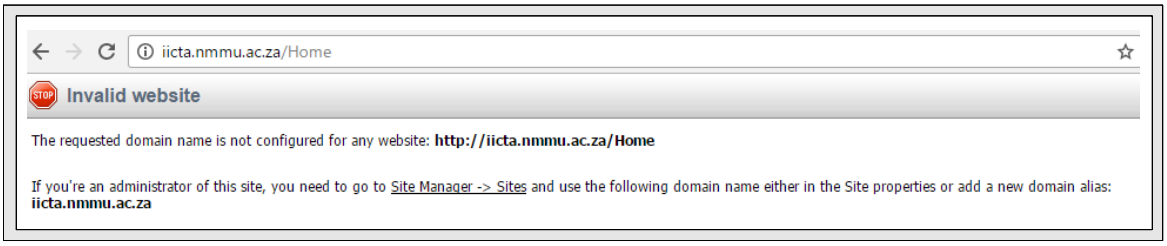


Figure 38. SACSAA members tab

The NMMU link on the SACSAA website directs users to an invalid website address (http://iicta.nmmu.ac.za/Home). However, a Google search leads to the NMMU Centre for Research in Information and Cyber Security (CRICS) website (http://crics.nmmu.ac.za/), which states that IICTA, the link provided on the SACSAA website, was closed in 2013 and replaced with CRICS in 2015.



The requested domain name is not configured for any website: **http://iicta.nmmu.ac.za/Home**

If you're an administrator of this site, you need to go to Site Manager -> Sites and use the following domain name either in the Site properties or add a new domain alias: **iicta.nmmu.ac.za**

Figure 39. Invalid IICTA website

The SACSAA website does not include up-to-date information on all the initiatives that members are involved with. CRICS members, for instance, developed a snakes and ladders cyber-security game (Reid & Van Niekerk, 2014a), but there is no information available on the SACSAA site about the game. The game does, however, appear in a picture of the free primary school curriculum (Figure 40).

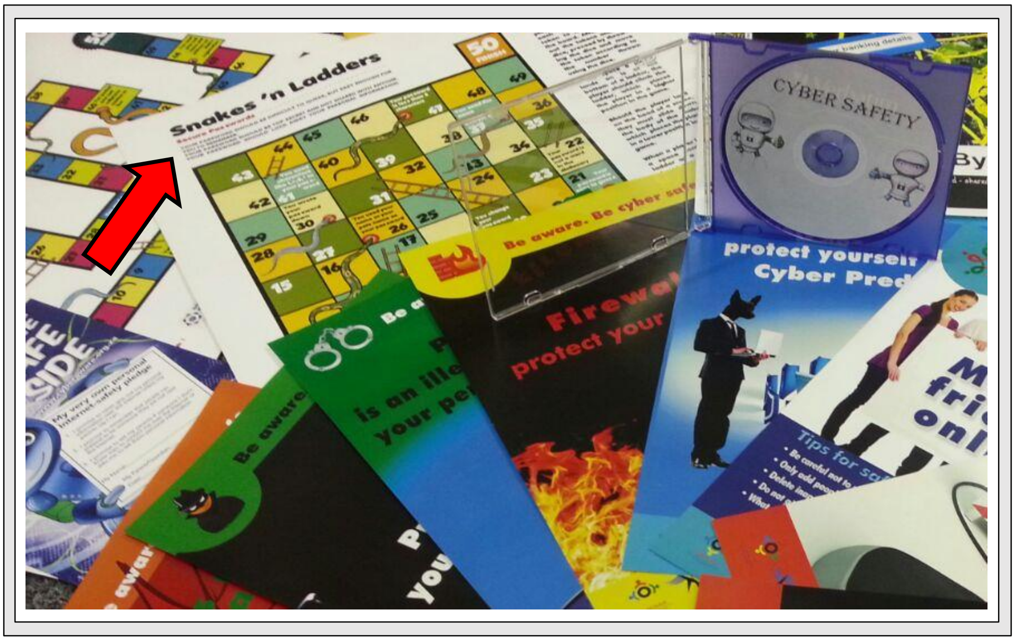
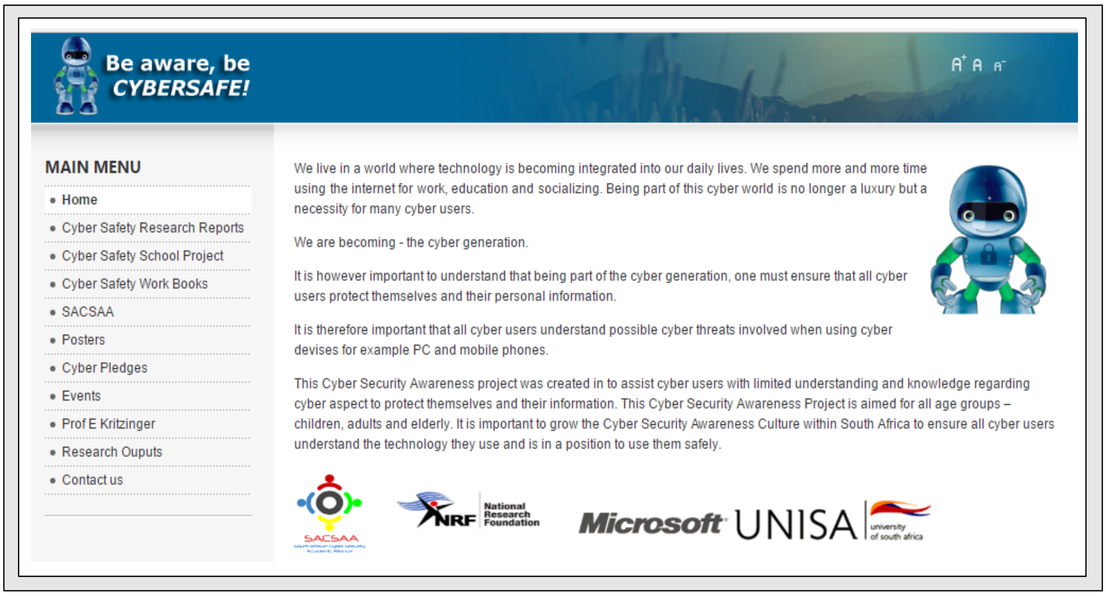


Figure 40. Snakes and ladders game

The link to the UNISA site (http://eagle.unisa.ac.za/elmarie/) provides access to cyber-safety research reports on South African schools and learners, and information about the cyber-safety school project (Figure 41).



We live in a world where technology is becoming integrated into our daily lives. We spend more and more time using the internet for work, education and socializing. Being part of this cyber world is no longer a luxury but a necessity for many cyber users.

We are becoming - the cyber generation.

It is however important to understand that being part of the cyber generation, one must ensure that all cyber users protect themselves and their personal information.

It is therefore important that all cyber users understand possible cyber threats involved when using cyber devises for example PC and mobile phones.

This Cyber Security Awareness project was created in to assist cyber users with limited understanding and knowledge regarding cyber aspect to protect themselves and their information. This Cyber Security Awareness Project is aimed for all age groups – children, adults and elderly. It is important to grow the Cyber Security Awareness Culture within South Africa to ensure all cyber users understand the technology they use and is in a position to use them safely.

Figure 41. Link to UNISA site

The SACSAA material is aimed at different target audiences, as the Alliance seeks to reach various stakeholders through their initiatives. The SACSAA workbooks for children (Figure 42) refers to the C3 topics and include information about cyber-security, cyber-safety and cyber-ethics (Kritzinger, 2012).

Download the workbooks:

- English:
- Sesotho:
- IsiZulu:
- Afrikaans:
- Children Edition:

Be aware. Be cyber safe
CYBER SECURITY AWARENESS WORKBOOK
Be aware. Be cyber safe
PUKUTIRO YA TEMOŠO YA TŠHIRELETŠEGO TŠHOMIŠONG YA INTHANETE
CYBER SECURITY AWARENESS WORKBOOK
SESOTHO SA LEBOWA
Be aware. Be cyber safe
INCWAJANA YOKUSEBENZELA EQWASHISA NGOKUVIKELEKA KOHLELOXHUMANO NGESIQOQELALWAZI
ISIZULU
Help kuberafknouery stopsit
WERKBOEK VIR DIE BEWUSTHEID VAN KUBERSEKURITEIT
Children Edition
Be aware. Be cyber safe
CYBER SECURITY AWARENESS WORKBOOK
NRF
Microsoft
UNISA

Figure 42. Cyber security awareness workbook

The target audience for the workbook was identified as school learners and teachers, but the following examples indicate that content is often more geared towards parents and teachers than towards children (Kritzinger, 2012). The workbook presents several topics, which are relevant to children; but it tries to accommodate the needs of children, parents and teachers, which means the focus on addressing children shifts throughout the workbook. Although the introduction states that the workbook was developed for school learners and educators, some sections are addressed specifically to parents (Kritzinger, 2012). These sections include gaming tips, and guidelines to teach young children and older children about online threats. Reference to online shopping, online banking and disclosure of financial information is more relevant to parents or adults (Kritzinger, 2012).

The following example, drawn from the workbook, indicates that the intention is to explain the behaviour of children to parents or educators:

> "In some cases, children and young people deliberately access inappropriate material, particularly as they move into adolescence. This can be done out of curiosity, or to share with peers in the 'shock value' of the content" (Kritzinger, 2012).

Guidelines are given to parents in the following extract from the workbook:

> "Explore your child's favourite websites. In general, it is useful to consider whether you are comfortable with the content of the sites and the potential for contact with others, including teens and adults. Is your child socially ready to manage contact from potentially ill-meaning strangers?" (Kritzinger, 2012).

Parents are alerted to behaviour changes of children in the following example, again drawn from the workbook:

> "If your child shows changes in behaviour or moods that are concerning, including changes in friendship groups, anxiety, sadness, clinginess or withdrawal, explore your concerns with him/her; and if necessary, seek professional support" (Kritzinger, 2012).

The cyber-security awareness workbook is available in English, Afrikaans, Sesotho, and isiZulu, which points to an attempt to accommodate target audiences of different languages. A child-friendly edition of the workbook has been added to the editions on the UNISA website. Elements of the workbook, such as posters and cyber pledges, are also available to download separately.

The SACSAA website does not provide an indication of how many schools have been assisted with cyber-security awareness initiatives and where these schools are located. Although the SACSAA website indicates that school visits are limited to the Nelson Mandela Bay Metropolitan Area (Reid & Van Niekerk, 2014b), photographs on the UNISA website shows that researchers from the partner university have also conducted school visits in 2015.

Apart from the workbook and safety pledge on the UNISA site, not many resources are available for children on the main SACSAA website. If SACSAA has been running campaigns for schools since 2011, the website is not reflecting all these campaigns. The only aspect of SACSAA campaigns which have been added to the website since 2011 are poster competition flyers and winning competition entries. As at November 2016, the 2016 poster information is not available on the site. The website contains outdated invalid links, content which appears only on external UNISA and UJ pages, and material which is designed according to different branding guidelines.

The UJ link directs users to the University of Johannesburg Centre for Cyber-security (http://adam.uj.ac.za/csi/index.html). Figure 43 indicates that the site provides cyber users with the opportunity to report cybercrime and has several up-to-date cyber-security articles, news snippets and links to media coverage.

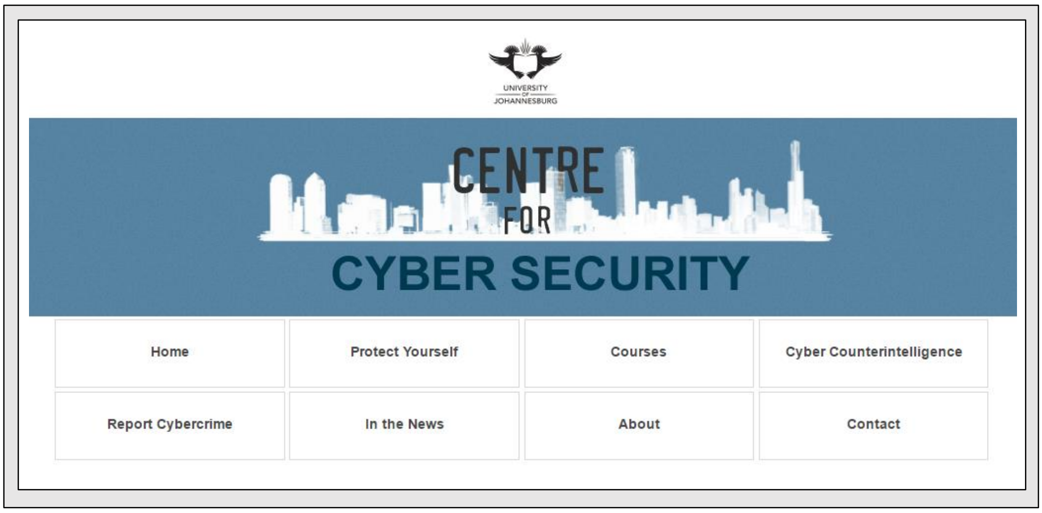
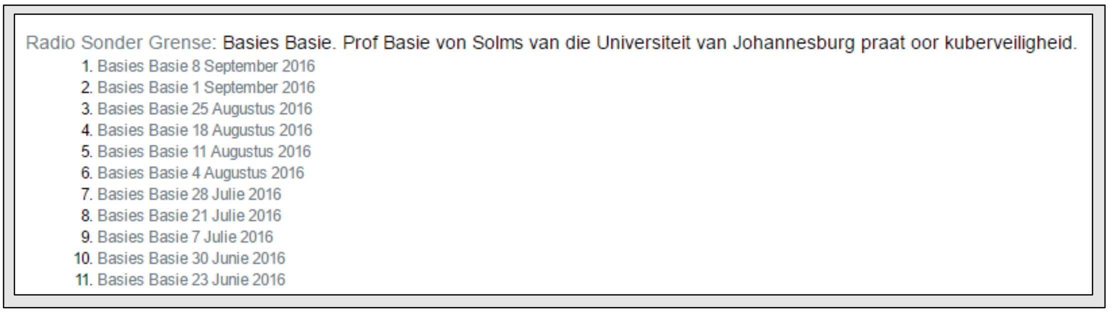


Figure 43. UJ Centre for Cyber Security website

Links to podcasts from the Basies Basie talkshow on Radio Sonder Grense, an Afrikaans radio station targeting listeners aged 35-49 (Leonard, 2014), is also provided as illustrated by Figure 44. The site is also directed to the Information Technology or cyber-security industry, as it provides information about training programmes and cyber counterintelligence research.



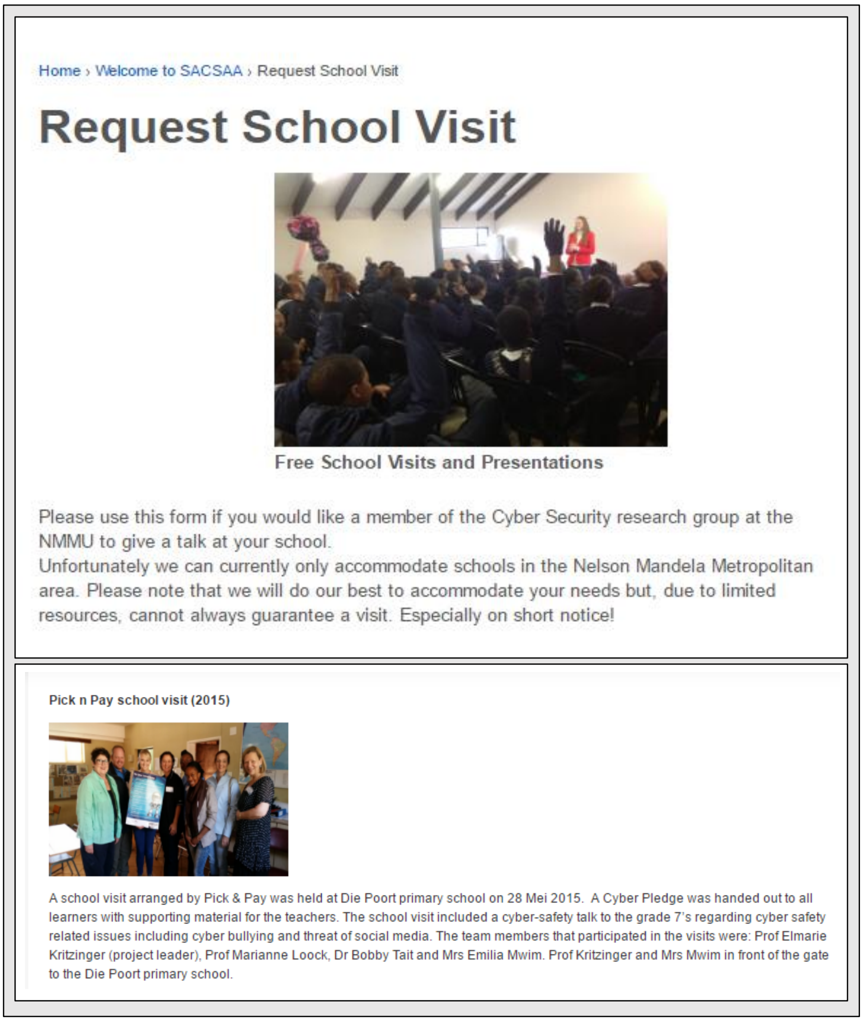
Radio Sonder Grense: Basies Basie. Prof Basie von Solms van die Universiteit van Johannesburg praat oor kuberveiligheid.

1. Basies Basie 8 September 2016
2. Basies Basie 1 September 2016
3. Basies Basie 25 Augustus 2016
4. Basies Basie 18 Augustus 2016
5. Basies Basie 11 Augustus 2016
6. Basies Basie 4 Augustus 2016
7. Basies Basie 28 Julie 2016
8. Basies Basie 21 Julie 2016
9. Basies Basie 7 Julie 2016
10. Basies Basie 30 Junie 2016
11. Basies Basie 23 Junie 2016

Figure 44. Basies Basie podcasts

5.9.8 Request school visit tab

Schools are invited to request a school visit if they are located in the Nelson Mandela Metropolitan area (Figure 45).



Home › Welcome to SACSAA › Request School Visit

Request School Visit

Free School Visits and Presentations

Please use this form if you would like a member of the Cyber Security research group at the NMMU to give a talk at your school.
Unfortunately we can currently only accommodate schools in the Nelson Mandela Metropolitan area. Please note that we will do our best to accommodate your needs but, due to limited resources, cannot always guarantee a visit. Especially on short notice!

Pick n Pay school visit (2015)

A school visit arranged by Pick & Pay was held at Die Poort primary school on 28 Mei 2015. A Cyber Pledge was handed out to all learners with supporting material for the teachers. The school visit included a cyber-safety talk to the grade 7's regarding cyber safety related issues including cyber bullying and threat of social media. The team members that participated in the visits were: Prof Elmarie Kritzinger (project leader), Prof Marianne Loock, Dr Bobby Tait and Mrs Emilia Mwim. Prof Kritzinger and Mrs Mwim in front of the gate to the Die Poort primary school.

Figure 45. School visits

In concluding this section, Stage Five of the framework deals with the execution of the campaign. Implementation is monitored to make adjustments when needed, and to report on the successes and areas of improvement for future campaigns. Stage Five was partially implemented by SACSAA, because success and areas of improvement link back to the campaign objectives. There are no clear objectives and timelines to indicate the different campaigns, which makes monitoring and reporting challenging. This challenge is further addressed as part of the SWOT analysis in the next section.

5.10 SWOT analysis

Based on the analysis of the SACSAA campaign, the following strengths, weaknesses, opportunities and threats are outlined (Table 7).

Table 7. SWOT analysis of SACSAA campaign

Strenghts of SACSAA campaign	Weaknesses of SACSAA campaign
• Exisiting material • Established poster competition • Expertise of members compiling campaigns • Exisiting mascots, Cyber Sid and Cyber Sindi	• SACSAA website • SACSAA branding • Campaign integration • SACSAA use of social media tools • Not reaching all target audiences
Opportunities for SACSAA campaign	**Threats for SACSAA campaign**
• Developing and improving SACSAA website • Development of clear brand guidelines • More collaboration between universities • More integration of campaign material • Integrating a social media strategy • Analysis of key target audiences and realignment of programme objectives	• Developing and aligning campaign material to campaign topics instead of target audience • Strong reliance on traditional communication channels to communicate with stakeholders

5.10.1 Strengths

The biggest strength for the SACSAA campaign is the updated cyber-security knowledge of researchers affiliated with the Alliance. The existing campaign material, such as the workbook and cyberpledge, was developed by cyber-security experts and addresses the C3 topics required to promote responsible digital citizenship. The material contains visual elements, uses colour effectively, and reinforces message content through the inclusion of activities which require participation from children. Participation in the poster competition has increased since its inception and indicates that children internalise messages received. The initiatives are further enhanced by the inclusion and development of campaign mascots, Cyber Sid and Cyber Sindi.

5.10.2 Weaknesses

Although some of the existing campaign material can be seen as a strength, the intended audiences may not be reached effectively with all the materials. The focus on campaign topics places the importance on campaign content and not on how the content addresses the needs of the audience. Exisiting campaign material refers the audience to the SACSAA website, which is outdated and contains limited resources. The SACSAA website and restricted social media tool utilisation further contributes to detract from the online reputation of the Alliance. The lack of clear branding guidelines unintentionally impacts on the growth of the SACSAA brand and brand support. Successful campaign integration requires branding guidelines and an understanding of the role of individual universities in relation to the overall purpose of SACSAA.

5.10.3 Threats

If the SACSAA website does not contain updated resources which meet the informational needs of target audiences, the SACSAA website may cause more damage to the SACSAA brand, which is still in its developmental phase. Campaigns require two-way communication and participation with target audiences, which extends to social media platforms. Campaign integration not only refers to collaboration between partner universities, but also to the integration of different media channels.

5.10.4 Opportunities

SACSAA has an existing website which can be further developed and maintained. More resources can be created, making use of clear brand and collaboration guidelines between universities. Clearly defining key target audiences and realigning programme objectives, according to the needs of these audiences, can lead to more integration of campaign material and to new campaign strategies. New campaign strategies can include the integration of a strategic social media strategy.

5.11 Conclusion

The purpose of Chapter Five was to analyse the SACSAA campaign according to the existing preparation and delivery layer of the cyber-security awareness and education framework and the proposed refined framework.

The existing preparation layer considered topic, medium, content and tool selection. The existing delivery layer identified the audience and the roles fulfilled by the audience. Based on the SACSAA campaign material, it can be concluded that the existing layers were implemented by SACSAA.

The refined preparation layer contains four stages, which start with a situational analysis during Stage One, followed by defining the target audience during Stage Two. Stage Three involves determining the campaign objectives and resources allocated to reach the objectives. Campaign objectives are developed into a communication strategy during Stage Four, which considers media channel selection, message design and the implementation plan. The refined delivery layer contains Stage Five, which includes campaign implementation, monitoring, adjustment and reporting. Based on the SACSAA campaign material, it can be concluded that a situational analysis was conducted and Stage One was implemented. Stages Two to Five were partially implemented by the Alliance. Analysis identified elements which were not included or which requires further development.

Based on the analysis of the SACSAA campaign, an overview of the strengths and weaknesses of the current campaign, and possible threats and opportunities for future campaigns were identified. The results of the SWOT analysis willl be used in Chapter Six to develop recommendations for the Alliance.

CHAPTER 6 FINDINGS AND RECOMMENDATIONS

"Begin at the beginning, and go on till you come to the end: then stop."

(Lewis Carroll, Alice's Adventures in Wonderland)

Entry vignette Abstract		
Introduction to case and context Chapter one: Introduction **Research question:** What are the elements required for the preparation and delivery of a cyber-safety awareness campaign?		
Chapter two: Research methodology		
Research objective I. To identify, using existing literature, the essential elements required for conducting a cyber-safety awareness campaign in South Africa.	**Description of case and context**	
	Chapter three: Cyber-safety in South Africa	Chapter four: Campaign planning
	Information Technology perspective	*Communication Science perspective*
Research objective II. To describe an existing South African cyber-safety awareness campaign aimed at schools, which forms the single case study;	**Development and detail about selected of issues** Chapter five: SACSAA campaign	
Research objective III. To compare the case study with the identified elements, and to determine whether there are any application gaps and areas for improvement;		
Research objective IV. To make recommendations for improved and integrated strategies for cyber awareness campaigns in South Africa.	**Lessons learnt and closing vignette** Chapter Six: Conclusion Findings and recommendations	

6.1 Introduction

The purpose of Chapter Six is to provide an overview of the study, to present recommendations for SACSAA, and to propose refinements to the preparation and delivery layer of the cyber-safety awareness and educational framework for South Africa. The chapter concludes with a summary of the contributions made by this study and a discussion of future research.

6.2 Chapter overview

Chapter one provided an overview of the factors which lead to increased cyber-security awareness needs. Active participating, working and engaging in cyber space is the norm for many in the contemporary world. The cyber world brings many advantages, but also it comes with risks. These risks know no bounds or age restrictions and can affect all users. Being aware of the risks and acting responsibly online contribute to creating a cyber-safety culture. Children grow up as digital citizens and should be prepared to function responsibly in the cyber world. To reach children, awareness and educational campaigns need to be developed and require collaboration amongst the principal role players, such as the teachers, schools and the Department of Basic Education, while taking the context of urban, suburban, township and rural living in South Africa into consideration.

To coordinate and integrate different cyber-security awareness initiatives, Kortjan and Von Solms (2014) developed a South African framework for cyber-safety awareness and education efforts. The five-layer framework consists of a strategic, tactical, preparation, delivery, and monitoring layer, supported by people, information, applications, infrastructure and financial capital (Kortjan, 2013). During a preliminary analysis of the framework, it was noted that campaign topics, content, mediums, and tools were selected during the preparation layer of the framework for an audience which was only described in the next layer, called the delivery layer. Communication research motivates for the identification of a target audience before developing campaign material (Dooley, Jones & Iverson, 2012; Ferguson & Phau, 2013; Mayasari, 2012; Nathanail & Adamos, 2013; Thaler & Helmig, 2013) to plan and execute cyber-safety and awareness campaigns efficiently (Aloul, 2012; Kajzer et al., 2014).

The preparation and delivery layers of the framework, therefore, required further refinement to ensure that it is practically implementable. This provided the basis for the purpose of the research. The study aimed to refine the preparation and delivery layers of the proposed cyber-safety awareness and educational framework for South Africa, as developed by Kortjan and Von Solms (2014), through the integration of communication theory. To refine the scope of the research and to ensure that the study provides a clear contribution to the field, the focus was on children (as they form the target audience for iWise-Mzanzi: for schools, which is a sub-campaign of the framework).

To fulfil the purpose of the study, the following research question was posed: What are the elements required for the preparation and delivery of a cyber-safety awareness campaign aimed at children?

To answer the research question, four objectives were set:

I. To identify, using the existing literature, the essential elements required for conducting a cyber-safety awareness campaign for children;

II. To describe an existing South African cyber-safety awareness campaign aimed at schools, which forms the single case study;

III. To compare the case study with the identified elements, and to determine whether there are any application gaps and areas for improvement;

IV. To make recommendations for improved and integrated strategies for cyber-awareness campaigns aimed at school children in South Africa.

To fulfil the research objectives of the study, a qualitative research design was adopted and discussed in chapter two.

Chapter two formed the methodological foundation of the study, as it contained the research design selected to meet the research objectives. The chapter provided an overview of the procedure followed for the study, which was first to identify the SACSAA cyber-safety campaign as a bounded system for the study. Secondly, data relevant to the purpose of the study needs was collected. Existing literature assisted in identifying the key elements required for carrying out a cyber-safety awareness campaign for children, through document analysis in Chapters Three and Four. The key elements, which formed the themes of the case study, were used to develop proposed changes to the existing preparation and delivery layers of the framework. Next, in Chapter Five, the refined framework layers were compared to the current framework layers through the SACSAA case study. The comparison led to the development of a SWOT analysis, which assisted in developing recommendations for SACSAA and the refinement of the framework in chapter six.

Chapter three discussed the elements contained in the preparation and delivery layer of the proposed cyber-safety education framework. The preparation layer includes topic, content, medium and tools. The chapter provided an overview of the different types of risks associated with online behaviour. The overview followed with a discussion of topics and content used to promote responsible online behaviour. The chapter discussed a holistic approach to cyber-security awareness to teach children about digital citizenship, which includes knowledge about cyber-security, cyber-safety and cyber-ethics. To convey cyber-security information to the intended audience, medium and tool selection is important. The delivery layer of the framework identified the target audience and their roles as educator and learner in the knowledge exchange. The chapter discussed the advantages and challenges experienced currently by campaign planners when trying to communicate with the intended audiences. This discussion was followed by chapter four, which considered the integration of communication theory in campaign planning and implementation.

Chapter four introduced basic models of communication to indicate the elements required for effective communication to take place during an exchange. The discussion was followed by a summary of the campaign principles proposed by Wilcox and Cameron (2014), program and campaign planning framework proposed by Cornelissen (2014), social marketing campaign planning steps proposed by Perloff (2014), the PRISA seven step programme (Skinner, Mersham & Benecke, 2013) the comprehensive planning tool proposed by Gregory (2010) and the steps in developing effective communication proposed by Kotler, Armstrong and Tait (2010). From the discussion, the following elements or themes were identified as essential for the preparation layer of the framework: situational analysis, identification of communication objectives, clearly defined target audience, and communication and implementation strategy. Implementation, monitoring and adjustment, as well as reporting, were identified as essential elements of the delivery layer. To verify the suggested refinements, chapter five introduced the SACSAA educational campaign aimed at schools.

Chapter five started with an overview of the development of SACSAA. The current South African cyber-safety awareness campaign aimed at schools, developed by SACSAA, formed the single case study. The campaign was analysed according to the implementation of the current and proposed refined preparation and delivery layers. The analysis, led to the identification of the strengths and weaknesses of the current campaign and proposed opportunities and threats of future campaigns, which forms the basis for the following recommendations.

6.3 Recommendations for SACSAA campaign planning

Table 8 provides an overview of the stages contained in the proposed refined preparation and delivery layers of the current cyber-security awareness and education framework.

Table 8. Planning stages in the refined preparation and delivery layer

Layer	**Stage**	**Proposed activity during stage**
Preparation	**One**	Situational Analysis
	Two	Define target audience
	Three	Determine campaign objectives and resources allocated
	Four	Formulate communication strategy • Media channel selection • Design message (content, structure, format, source) • Implementation plan (time schedule, stakeholder roles)
Delivery layer	**Five**	• Implement campaign in collaboration with stakeholders • Monitoring and adjustment • Reporting

The following recommendations are made for the preparation and delivery layers of the SACSAA campaign:

6.3.1 Stage one recommendations

With regard to a situational analysis, SACSAA needs to consider the specific needs of the audience, school or institution, based on its context. Although cyber-security, safety and ethics topics are relevant to all users, schools and learners at different ages may experience unique situations which require unique approaches. The location of the school and its management, would, for instance, impact the resources at its disposal. This, in turn, will influence the communication approach which will be used to reach the target audience.

A clear strategic direction is required to build the SACSAA brand, which will assist in building its trustworthiness. The services of a brand agency can assist the Alliance in developing and establishing a clear brand identity and design guidelines for future material.

6.3.2 Stage two recommendations

Regarding defining the audience, it is recommended that SACSAA clearly defines their target audiences according to demographic and psychographic characteristics. When developing materials for campaigns, it is important to consider the purpose and target audience in mind. Trying to reach several audiences with one document or resource often leads to information overload and message confusion, which results in ineffective communication. It is therefore recommended that SACSAA reviews current campaign material with the intended audience in mind and develops different resources to address the need for each target audience group.

SACSAA has already moved towards this approach by introducing another version of its workbook, which contains more activities to allow participation for children. Ideally, the workbook can be developed further into different publications and presented at a level appropriate to the needs of the audiences. Although several aspects of the workbook will overlap for different audiences, the way in which the content will be presented should be different, as it is addressed to different audiences. A separate workbook for parents or guardians can contain, for instance, more guidelines for technology in the home and incorporate digital citizenship as part of home values. A workbook for teachers and schools can contain guidelines for proactively dealing with online behaviour incidents and fostering a cyber safe culture at schools.

6.3.3 Stage three recommendations

Regarding communication objectives, it is recommended that SACSAA develops clear short-term objectives for each campaign. Objectives are used to develop a communication strategy and influence the way in which campaign success will be measured.

6.3.4 Stage four recommendations

Regarding formulating a communication strategy, it is recommended that partner universities clarify the purpose of the Alliance and decide on how more collaborative approaches can be used to build the SACSAA brand.

The Alliance has taken on a big challenge and faces an ever-changing cyber world. Although the existing initiatives have made a positive contribution to creating a cyber-safe culture, more communication from SACSAA regarding these initiatives are required. Technology and people constantly develop and change, which requires communication strategies and initiatives to adapt and change. Developing the SACSAA website and using cyber tools such as social media platforms creatively to communicate about cyber risks should be investigated further. The process should be completed in collaboration with key stakeholders who take on the duties as educator and learner (Kortjan, 2014).

6.3.5 Stage five recommendations

Regarding the implementation plan, it is recommended that SACSAA has timelines in place to distinguish between different campaigns. Campaigns are short-term in nature, and timelines should be aligned to the campaign objectives. When developing timelines, the roles and functions fulfilled by key stakeholders should also be considered.

Regarding monitoring and adjustment, it is recommended that SACSAA has clear campaign objectives which will assist in developing ways to monitor the implementation progress of campaigns and can assist in adjusting campaign strategies when needed.

Regarding reporting, it is recommended that SACSAA shares research results and reports of campaigns on the main SACSAA website, as it is currently only published on individual researcher or university websites.

6.4 Recommendations for SACSAA based on SWOT analysis

SACSAA has taken on the challenging task of creating a cyber safe culture in South Africa. Although the Alliance has made great strides through its current efforts aimed at children, the Alliance should consider the following recommendations, based on the strengths and weaknesses of the current SACSAA campaign, and possible threats and opportunities for future campaigns:

1. Develop clear branding guidelines which should be used for all material developed by SACSAA;
2. To build trust with the target audience, SACSAA needs to build its brand recognition.
3. Confirm the role of individual universities in relation to the overall purpose of SACSAA, the integration of campaigns and the use of SACSAA branding guidelines;
4. Appoint a content manager for SACSAA to ensure that all communication platforms are maintained;
5. Conduct a user experience evaluation of the existing SACSAA website, to assist with improving and developing it further;
6. Create more opportunities for two-way communication and participation of target audiences by incorporating the use of social media tools;
7. Define target audiences and set clear communication objectives for campaigns to ensure that audience needs are met;
8. Create and publish more resources on the SACSAA website for target audiences;
9. Newspaper clippings or media coverage obtained, should not only be placed on partner websites but should also be available for access on the SACSAA site to show that the Alliance is active; and
10. Integrate the campaign mascots, Cyber Sid and Cyber Sindi, more into efforts aimed at younger children.

Based on the analysis of the SACSAA campaign, the following recommendations are proposed for the refinement of the preparation and delivery layers of the existing five-layer cyber-security awareness and education framework.

6.5 Recommendations for framework

As indicated by Figure 46, the existing preparation layer consisted of topic, content, medium and tool selection. The existing delivery layer consisted of identifying the target audience and the roles fulfilled by the audience.

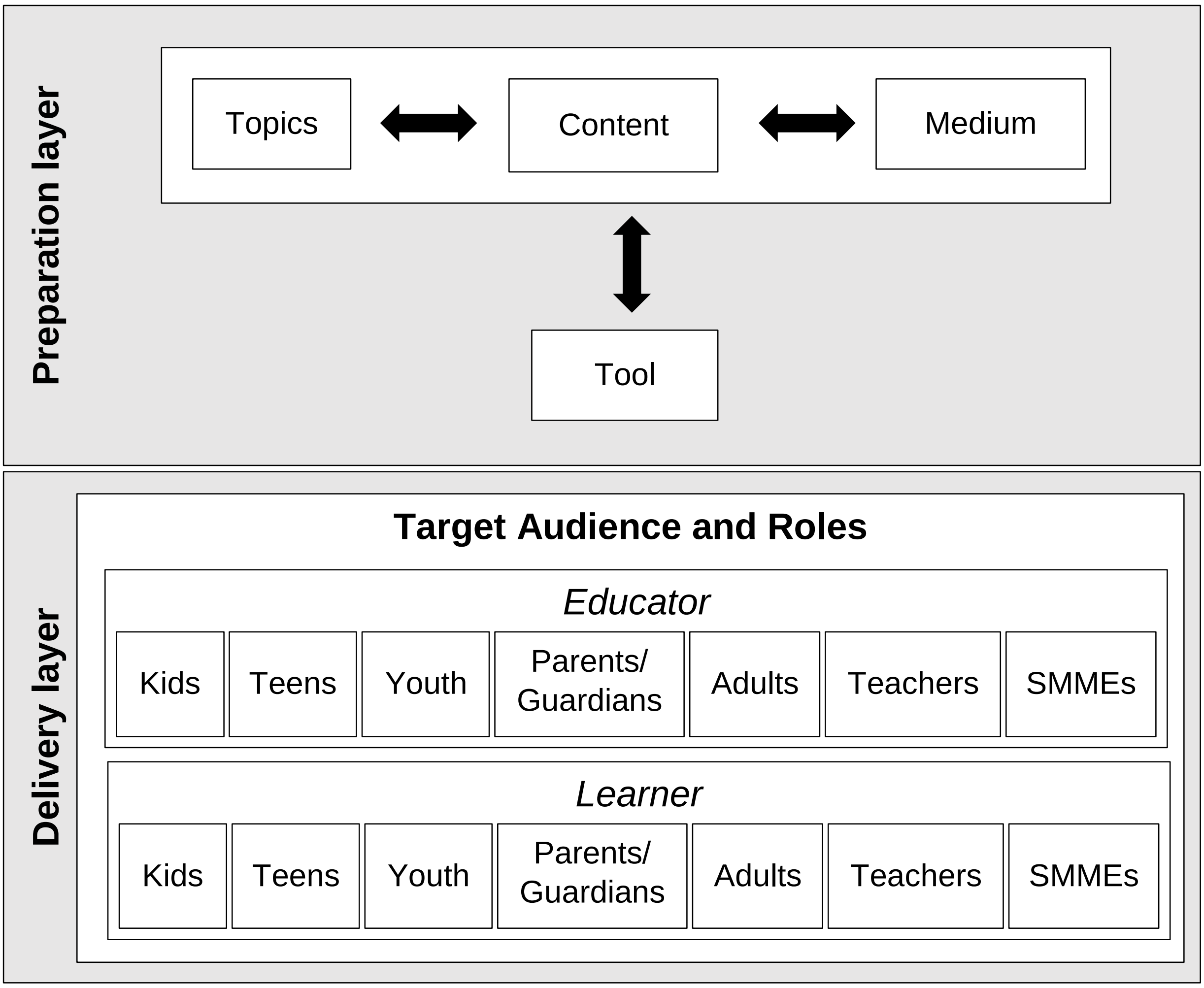


Figure 46. Existing preparation and delivery layer

The proposed refined layers are indicated by Figure 47.

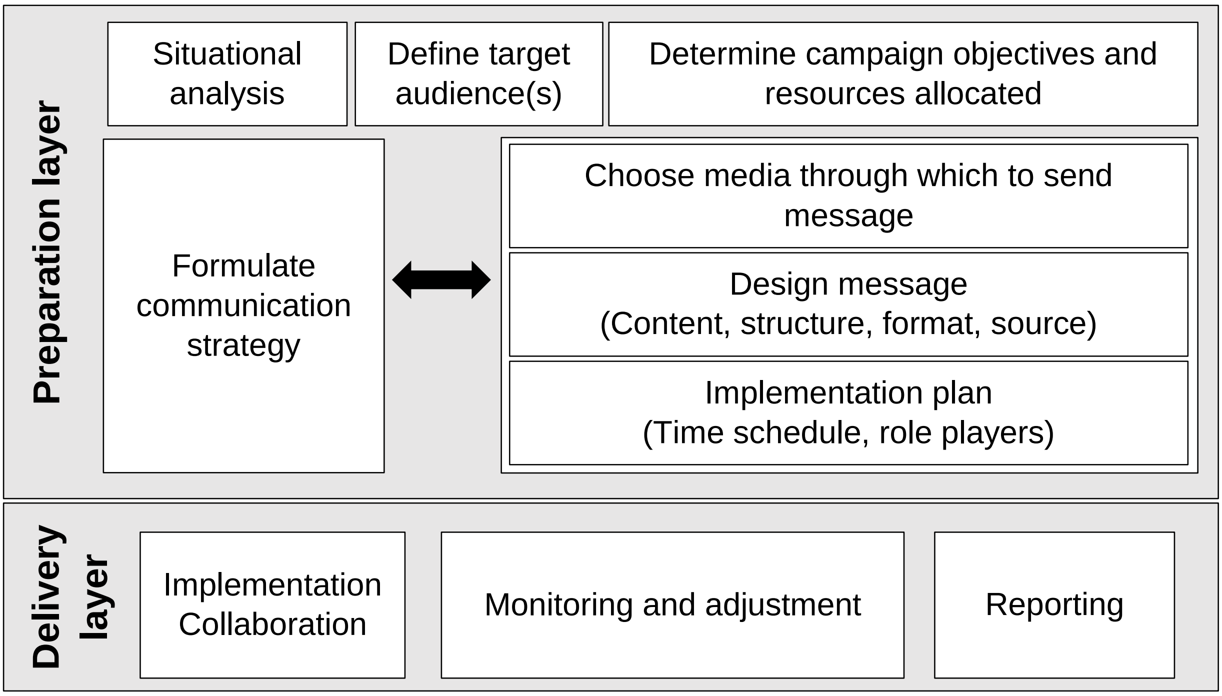

Preparation layer
Situational analysis
Define target audience(s)
Determine campaign objectives and resources allocated
Formulate communication strategy
Choose media through which to send message
Design message (Content, structure, format, source)
Implementation plan (Time schedule, role players)
Delivery layer
Implementation Collaboration
Monitoring and adjustment
Reporting

Figure 47. Refined preparation and delivery layer

The proposed refined preparation layer consists of a situational analysis, defining the target audience, determining resources allocated and formulating a communication strategy. The proposed refined delivery layer consists of campaign implementation, monitoring, and adjustment, as well as reporting on progress.

The target audience can range from a primary audience group, consisting of learners, to secondary target audiences, comprised of teachers, school management, and parents. Resources such as time, money, and staff members need to be considered when planning how to reach target audiences. The resources available will influence the strategy to reach the intended audiences.

All campaigns require an overall strategy guided by its purpose. Objectives are developed to guide the strategic direction of the campaign. The strategy influences the media selected to reach the target audience, the message design, and implementation plan. The target audience will affect the media selection. Campaign material will be designed to fit the media channel used. The implementation plan will set practical guidelines and timeframes in place to reach campaign objectives. During the formulation stage of the campaign strategy, the monitoring and evaluation of each communication tool will be planned to ensure that the objectives are measurable during the delivery layer of the framework.

Once the campaign is implemented, active monitoring and evaluation are required to make sure that adjustments are made as needed. Reporting of adjustments, successes, and areas of concern need to take place according to the planned schedule.

6.6 Closing vignette

The lack of cyber-safety awareness is one of the major cyber-security concerns in South-Africa (Kritzinger, 2014; Swart, Irwin & Grobler, 2014). Although schools and children in South Africa are faced with many context-specific and general challenges (Maringe, Masinire & Nkambule, 2015), key stakeholders can work together to ensure that children are equipped with the skills required to function as responsible digital citizens. Digital citizenship and knowledge about cyber-ethics, cyber-safety and cyber-security can be conveyed to children through awareness and educational campaigns.

To provide structure to cyber awareness and educational initiatives in South Africa, Kortjan and Von Solms (2014) developed a five-layer cyber-security awareness and education framework. The framework consisted of a strategic, tactical, preparation, delivery, and monitoring layer, supported by people, information, applications, infrastructure and financial capital (Kortjan, 2013). Initial analysis revealed that the existing preparation layer and delivery layer required further development. The preparation layer, which consisted of topic, content, medium and tool selection, required the campaign planner to make strategic choices which should be based on the intended audience. The audience, however, was not defined during the preparation layer, as the framework required the campaign planner to identifying the target audience and the roles fulfilled by the audience, in the next layer (the delivery layer).

The purpose of the study was, therefore, to refine the preparation and delivery layers of the proposed cyber-safety awareness and educational framework for South Africa, as developed by Kortjan and Von Solms (2014), through the integration of communication theory. The intent of refining the layers was to ensure that the framework can be implemented practically.

To refine the scope of the research and to ensure that the study provided a clear contribution to the field, the focus was on children as they form the target audience for iWise-Mzanzi: For Schools, which was a sub-campaign of the framework developed by Kortjan and Von Solms (2014).

A qualitative research approach was used to address the following objectives of the study:

Research Objective I

The first research objective was to identify, using the existing literature, the essential elements required for conducting a cyber-safety awareness campaign for children. Chapter three of the dissertation explores the essential elements required to conduct a cyber-safety awareness campaign for children. The move towards digital citizenship, supported by C3 topics (cyber-ethics, cyber-security and cyber-safety) was seen as essential. From a communication perspective, six campaign planning models are reviewed and formed the theoretical lens for the study. Chapter four of the dissertation explored the requirements for campaign planning from a communication perspective. The essential campaign development stages include situational analysis, defining the target audience, developing communication objectives and determine resources available, developing a communication strategy, implementation, and evaluation.

Research Objective II

The second research objective was to compare an existing South African cyber-safety awareness campaign aimed at schools, with the current and refined cyber-security awareness frameworks. The SACSAA campaign formed the case study for the research and campaign material was analysed according to the existing and proposed refined framework.

Research Objective III

The third research objective was to provide recommendations for improved and integrated strategies for cyber-awareness campaigns aimed at children in South Africa, based on research objective I and II. The recommendations are discussed in Chapter Six.

6.7 Summary of contributions

From a theoretical perspective, the interdisciplinary study contributed towards the refinement of the cyber-safety awareness and educational framework for South Africa, through the integration of communication theory. By incorporating theory from the field of communication, the existing preparation and delivery layers of the framework were further developed into five planning stages to assist in the practical implementation of the framework in future. From a practical perspective, the study made recommendations for SACSAA which will, in turn, assist the Alliance in developing their campaigns further.

Based on the study, the following questions can be used to guide the preparation and implementation of cyber-security campaigns aimed at children:

Table 9. Questions to guide planning stages

Layer	Stage	Questions to guide activity planning during each stage
Preparation	**One**	**Situational Analysis** • What is the situation of concern? • Why is the issue a concern? • Where is the issue of concern? • Who is of concern? • When is the issue of concern? • Whom are the stakeholders involved?

Table 9. Questions to guide planning stages (Continued)

Layer	Stage	Questions to guide activity planning during each stage
Preparation	**Two**	**Define target audience** • Which criteria will be used to define the target audience? • Who is the primary target audience of your campaign? • Who is the secondary target audience of your campaign? • What do you know about the primary/ secondary target audience? • What are the needs of the primary/ secondary target audience? • How can you address the needs of the primary/ secondary target audience? • Where will you find the primary/ secondary target audience? • How will you reach the primary/ secondary target audience? • When can you reach the primary/ secondary target audience?
	Three	**Determine campaign objectives and resources allocated** • What is the purpose of the campaign? • Why do you want to develop the campaign? • How will the campaign address the issue(s) of concern? • How much funding is available for the campaign? • Do you have the skills required to develop and implement all aspects of the campaign or should experts be appointed to assist? • Do your objectives adhere to SMARTA principles? ○ Specific ○ Measurable ○ Attainable ○ Realistic ○ Time-bound ○ Adjustable

Table 9. Questions to guide planning stages (Continued)

Layer	Stage	Questions to guide activity planning during each stage
Preparation	**Four**	**Formulate communication strategy** • Media channel selection o Which media channels are available within the budget allocated? o What are the advantages and limitations of the media channels? o How will the media channels assist in reaching the target audience? o Why are the selected media channel(s) the most suited to reach the target audience? o How will the media channels contribute towards reaching the campaign objectives? o When are the media channels available? • Design message (content, structure, format, source) o What is the key message for the target audience to remember? o Why should the target audience take note of the key message and content? o How can the key message be communicated to the target audience? o When can the key message be communicated? o What are the format and structure requirements for the media channel selected? o Who should be used as campaign source? o Would the source be seen as credible? o How will the key message be understood by the target audience? • Implementation plan (schedule, stakeholder roles) o Which activities are required for implementation? o When would the message be delivered to the target audience? o Who will deliver the message to the target audience? o Where will the message be delivered? o How will the message be delivered? o Which stakeholders are involved in implementing the campaign? o What are the roles played by stakeholders?

Table 9. Questions to guide planning stages (Continued)

Layer	Stage	Questions to guide activity planning during each stage
Delivery layer	**Five**	• **Implement campaign in collaboration with stakeholders** • **Monitoring and adjustment** • **Reporting** o How will campaign implementation be monitored? o When will campaign effectiveness be determined? o When will adjustments to the implementation plan be made? o When will campaign progress be reported? o How often will monitoring and evaluation of campaign initiatives take place? o Where will monitoring and evaluation take place? o Which measurement and evaluation principles will be used?

6.8 Future research

Research to determine the information needs of South African teachers and parents in urban, suburban, township and rural areas would be beneficial for campaign material development. Although the monitoring layer of the framework did not form part of the proposed research, existing literature referred to the importance of monitoring and evaluation. The current monitoring layer refers to benchmarking, success indication and periodic status reports. Measuring the campaign output by reviewing the campaign reach and audience feedback can assist in the development of future campaigns. Message design should also be evaluated regarding its persuasiveness and whether it has led to retention and behaviour change. Developing the monitoring layer is therefore suggested before implementing the framework.

REFERENCE LIST

Abawajy, J., 2014. User preference of cyber security awareness delivery methods. *Jounal of Behaviour & Information Technology*, Vol. 33(3), pp.236–247. [Online] Available at: http://dx.doi.org/10.1080/0144929X.2012.708787 [Accessed June 8, 2015].

Abbasi, S. & Manawar, M., 2011. Multi-dimensional challenges facing digital youth and their consequences. In *Cybersecurity Summit (WCS) Second Worldwide.* pp. 1–5. [Online] Available at: http://ieeexplore.ieee.org/document/5978784/ [Accessed June 8, 2015].

Aboujaoude, E., Savage, M.W., Starcevic, V. & Salame, W.O., 2015. Cyberbullying: Review of an old problem gone viral. *Journal of Adolescent Health*, Vol. 57(1), pp.10–18. [Online] Available at: http://dx.doi.org/10.1016/j.jadohealth.2015.04.011 [Accessed June 28, 2016].

Adegbenro, J. & Gumbo, M., 2014. Assessing Computer Application Technology teachers' e-skills and procedural knowledge with regard to teaching with ICT infrastructure. In *Proceedings of the 13th European Conference on E-Learning*. pp. 687–691. [Online] Available at: search.proquest.com/openview/d36727ee2470d07e9952b41321da8e8b/1?pq... [Accessed June 21, 2016].

Adesote, S.A. & Fatoki, O.R., 2013. The role of ICT in the teaching and learning of history in the 21st century. *Educational Research and Reviews*, Vol. 8(21), pp.2155–2159. [Online] Available at: http://www.academicjournals.org/article/article1383039843_Adesote and Fatoki.pdf [Accessed August 21, 2016].

Adetunji, R.. & Sze, K.P., 2012. Understanding non-verbal Communication across cultures : A symbolic interactionism approach. In *i-Come International Conference on Communication and Media.* pp. 1–8. [Online] Available at: https://ssrn.com/abstract=2178486 [Accessed November 29, 2015].

Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L. & O'Carroll, E., 2015. A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, Vol. 2041(March 2016), pp.1–19. [Online] Available at:

http://www.tandfonline.com/doi/abs/10.1080/21582041.2015.1117648 [Accessed June 13, 2016].

Akbari, M., 2015. Different impacts of advertising appeals on advertising attitude for high and low involvement products. *Global Business Review*, Vol. 16(3), pp.478–493. [Online] Available at: http://gbr.sagepub.com/cgi/doi/10.1177/0972150915569936 [Accessed June 2, 2016].

Aladwani, A.M., 2014. Gravitating towards Facebook (GoToFB): What it is? and How can it be measured? *Computers in Human Behavior*, Vol. 33, pp.270–278. [Online] Available at: http://dx.doi.org/10.1016/j.chb.2014.01.005 [Accessed June 28, 2016].

Alavi, N., Reshetukha, T. & Prost, E., 2015. Bullying including cyber bullying increases the risk of suicidal behaviour. *European Psychiatry*, Vol. 30(1), p.209. [Online] Available at: doi:10.1016/S0924-9338(15)30169-3 [Accessed June 7, 2016].

Alavi, R., Islam, S. & Mouratidis, H., 2016. An information security risk-driven investment model for analysing human factors. *Information & Computer Security*, Vol. 24(1), pp.1–22. [Online] Available at: eprints.brighton.ac.uk/16019/ [Accessed June 7, 2016].

Albrechtsen, E. & Hovden, J., 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers and Security*, Vol. 29(4), pp.432–445. [Online] Available at: http://dx.doi.org/10.1016/j.cose.2009.12.005 [Accessed June 28, 2016].

Al-Fedaghi, S., 2012. A conceptual foundation for the Shannon-Weaver Model of communication. *International Journal of Soft Computing*, Vol. 7(1), pp.12–19. [Online] Available at: www.medwelljournals.com/abstract/?doi=ijscomp.2012.12.19 [Accessed August 29, 2016].

Alhojailan, M.I. & Ibrahim, M., 2012. Thematic analysis: a critical review of its process and evaluation. *WEI International European AcademicConference Proceedings*, Vol. 1(2011), pp.8–21. [Online] Available at: fac.ksu.edu.sa/sites/default/files/ta_thematic_analysis_dr_mohammed_alhojailan.pdf [Accessed June 12, 2016].

Al-Jerbie, S.I. & Jali, M.Z., 2014. Second look at the Information Security awareness among secondary school students. In *The International Conference on Information Security and Cyber Forensics (InfoSec2014)*. pp. 88–97. [Online] Available at: http://sdiwc.net/digital-library/a-second-look-at-the-information-security-awareness-among-secondary-school-students [Accessed June 28, 2016].

Al-karaki, J., Harous, S., Al-muhairi, H., Alhammadi, Y., Ayyoub, S., Alzaabi, H., Alsalhi, M., Salem, S. & Alamiri, A., 2016. Towards an innovative Comptuer Science & Technology Curriculum in UAE public schools system. In *IEEE Global Engineering Education Conference (EDUCON)*. pp. 883–891. [Online] Available at: ieeexplore.ieee.org/iel7/7469053/7474513/07474656.pdf [Accessed June 29, 2016].

Al-Khateeb, H.M. & Epiphaniou, G., 2016. How technology can mitigate and counteract cyber-stalking and online grooming. *Computer Fraud and Security*, Vol. 2016(1), pp.14–18. [Online] Available at: www.sciencedirect.com/science/article/pii/S1361372316300082 [Accessed June 7, 2016].

Allais, S., 2012. Will skills save us? Rethinking the relationships between vocational education, skills development policies, and social policy in South Africa. *International Journal of Educational Development*, Vol. 32(5), pp.632–642. [Online] Available at: http://dx.doi.org/10.1016/j.ijedudev.2012.01.001 [Accessed August 21, 2015].

Aloufi, A.E.M., 2015. *A cognitive theory-based approach for the evaluation and enhancement of Internet security awareness among children aged 3-12 years.* [Online] Available at: scholarworks.rit.edu/theses/8821/ [Accessed June 28, 2016].

Aloul, F.A., 2012. The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, Vol. 3(3), pp.176–183. [Online] Available at: doi:10.4304/jait.3.3.176-183 [Accessed June 7, 2015].

Altman, M., Schöer, V. & Rama, N., 2013. Education and youth employment in Sub-Saharan countries: linkages and policy responses. In *African Economic Research Consortium workshop on Youth and Unemployment.* [Online] Available at:

https://www.gtac.gov.za/Research Repository/Education and Youth Employment in Sub-Sahara Africa Linkages and Policy Responses.pdf.

Amankwa, E., Loock, M. & Kritzinger, E., 2014. A conceptual analysis of information security education, information security training and information security awareness definitions. *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, pp.248–252. [Online] Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7038814 [Accessed February 25, 2016].

Amankwa, E., Loock, M. & Kritzinger, E., 2015. Enhancing Information Security education and awareness : proposed characteristics for a model. In *Second International Conference on Information Security and Cyber Forensics (InfoSec)*. pp. 72–77. [Online] Available at: ieeexplore.ieee.org/iel7/7431308/7435496/07435509.pdf [Accessed June 7, 2016].

Amichai-Hamburger, Y. & Vinitzky, G., 2010. Social network use and personality. *Computers in Human Behavior*, Vol. 26(6), pp.1289–1295. [Online] Available at: http://linkinghub.elsevier.com/retrieve/pii/S0747563210000580 [Accessed March 2, 2014].

Amod, Z., Vorster, A. & Lazarus, K., 2013. Attention-Deficit/Hyperactivity Disorder (ADHD) as a barrier to learning and development within the South African context: The perspectives of teachers. *InTech*, pp.215–241. [Online] Available at: http://dx.doi.org/10.5772/53784 [Accessed August 21, 2015].

Anand, S., 2014. Challenges in cross cultural marketing communication- effective approach using semiotic lens. *Global Journal of Finance and Management*, Vol. 6(9), pp.875–886. [Online] Available at: www.ripublication.com/gjfm-spl/gjfmv6n9_11.pdf [Accessed June 13, 2016].

Andersen, R.S., Vuori, J. a. & Guillaume, X., 2015. Chromatology of security: introducing colours to visual security studies. *Security Dialogue*, Vol. 46(5), pp.440–457. [Online] Available at: http://sdi.sagepub.com/cgi/doi/10.1177/0967010615585106 [Accessed June 13, 2016].

Andreu, L., Casado-Díaz, A.B. & Mattila, A.S., 2015. Effects of message appeal and service type in CSR communication strategies. *Journal of Business Research*, Vol. 68(7), pp.1488–1495. [Online] Available at: http://dx.doi.org/10.1016/j.jbusres.2015.01.039 [Accessed June 2, 2016].

Antonova, N.V., 2015. The psychological effectiveness of interactive advertising. *Journal of Creative Communications*, Vol. 10(3), pp.303–311. [Online] Available at: http://crc.sagepub.com/cgi/doi/10.1177/0973258615614426 [Accessed February 18, 2016].

Appel, M., Stiglbauer, B., Batinic, B. & Holtz, P., 2014. Internet use and verbal aggression: The moderating role of parents and peers. *Computers in Human Behavior*, Vol. 33, pp.235–241. [Online] Available at: http://dx.doi.org/10.1016/j.chb.2014.01.007 [Accessed June 28, 2015].

Ashenden, D., 2008. Information Security management: A human challenge? *Information Security Technical Report*, Vol. 13(4), pp.195–201. [Online] Available at: http://linkinghub.elsevier.com/retrieve/pii/S1363412708000484 [Accessed May 30, 2014].

Averbeck, J.M., Jones, A. & Robertson, K., 2011. Prior knowledge and health messages: An examination of affect as heuristics and information as systematic processing for fear appeals. *Southern Communication Journal*, Vol. 76(1), pp.35–54. [Online] Available at: www.tandfonline.com/doi/abs/10.1080/10417940902951824 [Accessed June 2, 2016].

Aydin, S., 2012. A review of research on Facebook as an educational environment. *Educational Technology Research and Development*, Vol. 60(6), pp.1093–1106. [Online] Available at: http://link.springer.com/10.1007/s11423-012-9260-7 [Accessed February 2, 2014].

Babooram, M., Mullan, B.A. & Sharpe, L., 2010. Children’s understandings of mediated health campaigns for childhood obesity. *Nutrition & Food Science*, Vol. 40(3), pp.289–298. [Online] Available at: www.emeraldinsight.com/doi/abs/10.1108/00346651011043989 [Accessed June 2, 2016].

Bada, M. & Sasse, A., 2014. *Cyber security awareness campaigns: Why do they fail to change behaviour?*, [Online] Available at:

http://www.cs.ox.ac.uk/publications/publication9343-abstract.html [Accessed June 16, 2016].

Bakar, H.S.A., 2015. The emergence themes of cyberbullying among adolescences. *International Journal of Adolescence and Youth*, Vol. 3843(March), pp.1–14. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/02673843.2014.992027 [Accessed June 21, 2016].

Balmer, J.M.T., 2012. Strategic corporate brand alignment: perspectives from identity based views of corporate brands. *European Journal of Marketing*, Vol. 46(7/8), pp.1064–1092. [Online] Available at: http://dx.doi.org/10.1108/03090561211230205 [Accessed March 14, 2015].

Bandhiya, D.B. & Joshi, A., 2015. Encompassing the scope of Western Models of communication. *PARIPEX Indian Journal of Research*, Vol. 4(9), pp.222–224. [Online] Available at: https://www.worldwidejournals.com/paripex/file.php?val=September_2015_1442223781__85.pdf [Accessed July 1, 2016].

Barbour, J.B. & Gill, R., 2014. Designing communication for the day-to-day safety oversight of nuclear power plants. *Journal of Applied Communication Research*, Vol. 42(2), pp.168–189. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/00909882.2013.859291 [Accessed June 26, 2016].

Bardach, D., Knyazeva, S. & Lane, A., 2012. *Introducing the opportunities and challenges of OER: the case of the Commonwealth of Independent States and Baltic States*, [Online] Available at: http://oro.open.ac.uk/33975/ [Accessed August 21, 2016].

Barker, R., 2013. Strategic integrated communication: An alternative perspective of integrated marketing communication? *Communicatio*, Vol. 39(1), pp.102–121. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/02500167.2013.741071 [Accessed June 25, 2015].

Barnard-Wills, D., 2012. E-safety education: Young people, surveillance and responsibility. *Criminology and Criminal Justice*, Vol. 12(3), pp.239–255. [Online]

Available at: 10.1177/1748895811432957 [Accessed June 28, 2016].

Bastos, W. & Levy, S.J., 2012. A history of the concept of branding: practice and theory. *Journal of Historical Research in Marketing*, Vol. 4(3), pp.347–368. [Online] Available at: http://dx.doi.org/10.1108/17557501211252934 [Accessed June 9, 2015].

Bayat, A., Louw, W. & Rena, R., 2014. The impact of socio-economic factors on the performance of selected high school learners in the Western Cape Province, South Africa. *Journal of Human Ecology*, Vol. 45(3), pp.183–196. [Online] Available at: www.krepublishers.com/.../JHE-45-3-183-14-2593-Rena-R-Tx[2].pmd.pdf [Accessed August 9, 2016].

Bendovschi, A., 2015. Cyber-Attacks – trends, patterns and security countermeasures. *Procedia Journal of Economics and Finance*, Vol. 28, pp.24–31. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S2212567115010771\nhttp://linkinghub.elsevier.com/retrieve/pii/S2212567115010771 [Accessed June 7, 2016].

Beneke, J., 2011. Student recruitment and relationship marketing- convergence or contortion? *South African Journal of Higher Education*, Vol. 25(3), pp.412–424. [Online] Available at: http://libaccess.mcmaster.ca/login?url=http://search.proquest.com/docview/1023529725?accountid=12347\nhttp://sfx.scholarsportal.info/mcmaster?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&sid=ProQ:ProQ:ericshell&atitle=Studen [Accessed June 9, 2015].

Bennett, W.L., Wells, C. & Rank, A., 2009. Young citizens and civic learning: two paradigms of citizenship in the digital age. *Citizenship Studies*, Vol. 13(2), pp.105–120. [Online] Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-70350020664&partnerID=tZOtx3y1 [Accessed July 1, 2016].

Berehoiu, S.T., Wohlfarth, H. & Sam, C., 2013. Considerations regarding use and role of colour in marketing. *Scientific Papers Series Management , Economic Engineering in Agriculture and Rural Development., Economic Engineering in Agriculture and Rural Development.*, Vol. 13(1), pp.269–274. [Online] Available at: http://managementjournal.usamv.ro/index.php/scientific-papers/252-

considerations-regarding-use-and-role-of-colour-in-marketing [Accessed July 1, 2016].

Bhana, D., 2012. Girls are not free — In and out of the South African school. *International Journal of Educational Development .*, Vol. 32, pp.352–358. [Online] Available at: 10.1016/j.ijedudev.2011.06.002 [Accessed August 7, 2016].

Bhana, D., 2015. When caring is not enough: The limits of teachers ' support for South African primary school-girls in the context of sexual violence. *International Journal of Educational Development*, Vol. 41, pp.262–270. [Online] Available at: http://dx.doi.org/10.1016/j.ijedudev.2014.08.003 [Accessed August 7, 2016].

Blombäck, A. & Ramírez-Pasillas, M., 2012. Exploring the logics of corporate brand identity formation. *Corporate Communications: An International Journal*, Vol. 17(1), pp.7–28. [Online] Available at: http://dx.doi.org/10.1108/13563281211196335 [Accessed April 9, 2015].

Blythe, J.M., 2013. Cyber security in the workplace : Understanding and promoting behaviour change. In *Doctoral Consortium. CH Italy.* [Online] Available at: http://ceur-ws.org [Accessed June 16, 2014].

Boblin, S.L., Ireland, S., Kirkpatrick, H. & Robertson, K., 2013. Using Stake's qualitative case study approach to explore implementation of evidence-based practice. *Qualitative health research*, Vol. 23(9), pp.1267–75. [Online] Available at: http://www.ncbi.nlm.nih.gov/pubmed/23925405 [Accessed February 18, 2016].

Bock, D.E., Poole, S.M. & Joseph, M., 2014. Does branding impact student recruitment: a critical evaluation. *Journal of Marketing for Higher Education*, Vol. 24(February 2015), pp.11–21. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/08841241.2014.908454 [Accessed June 9, 2015].

Boeriis, M. & Holsanova, J., 2012. Tracking visual segmentation: connecting semiotic and cognitive perspectives. *Visual Communication*, Vol. 11(3), pp.259–281. [Online] Available at: 10.1177/1470357212446408 [Accessed June 13, 2016].

Botha, A., Herselman, M. & van Greunen, D., 2010. Mobile user experience in a mlearning environment. *Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists* *on - SAICSIT '10*, (August 2016), pp.29–38. [Online] Available at: http://portal.acm.org/citation.cfm?doid=1899503.1899507 [Accessed August 21, 2016].

Bovina, I.B., Dvoryanchikov, N. V. & Budykin, S. V., 2014. Shared Meanings about Information Security of Children: An Exploratory Study. *Procedia - Social and Behavioral Sciences*, Vol. 146, pp.94–98. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S1877042814047466.

Bowen, G.A., 2009. Document analysis as a qualitative research method. *Qualitative Research Journal*, Vol. 9(2), pp.27–40. [Online] Available at: www.emeraldinsight.com/doi/abs/10.3316/QRJ0902027 [Accessed February 27, 2016].

Boyes, M.E., Bowes, L., Cluver, L.D., Ward, C.L. & Badcock, N.A., 2014. Bullying victimisation, internalising symptoms, and conduct problems in South African children and adolescents: A longitudinal investigation. *Journal of Abnormal Child Psychology*, Vol. 42(8), pp.1313–1324. [Online] Available at: 10.1007/s10802-014-9888-3 [Accessed August 21, 2016].

Brady, C., 2010. *Security awareness for children.* London: Royal Holloway University of London. Department of Mathematics. [Online] Available at: http://www.rhul.ac.uk/mathematics/techreports [Accessed June 23, 2014].

Breen, A., Daniels, K. & Tomlinson, M., 2015. Children's experiences of corporal punishment: A qualitative study in an urban township of South Africa. *Child abuse & neglect*, Vol. 48, pp.131–139. [Online] Available at: http://dx.doi.org/10.1016/j.chiabu.2015.04.022 [Accessed August 7, 2016].

Broll, R., 2014. *Policing cyber bullying: How parents, educators, and law enforcement respond to digital harassment.* [Online] Available at: http://ir.lib.uwo.ca/etd/2116/ [Accessed June 28, 2015].

Buono, L., 2014. Fighting cybercrime through prevention, outreach and awareness raising. *ERA Forum*, Vol. 15(1), pp.1–8. [Online] Available at: http://link.springer.com/article/10.1007/s12027-014-0333-4 [Accessed June 29, 2016].

Burridge, G., 2010. Raising a digital child: a digital citizenship handbook for parents.

Learning, Media & Technology, Vol. 35(3), pp.363–364. [Online] Available at: 10.1080/17439884.2010.481557\nhttp://0-search.ebscohost.com.mercury.concordia.ca/login.aspx?direct=true&db=a9h&AN=55475162&site=ehost-live&scope=site [Accessed July 1, 2016].

Burton, P. & Leoschut, L., 2013. *School violence in South Africa: Results of the 2012 National school violence study*, [Online] Available at: www.cjcp.org.za/school-violence-in-south-africa.html [Accessed August 21, 2016].

Butler, Z. & Howcroft, G., 2014. Cyber bullying among children and adolescents: A systematic review. *Proceedings of the African Cyber Citizenship Conference 2014 (ACC2014)*, Vol. 2014(November), pp.15–25. [Online] Available at: http://accc2014.nmmu.ac.za/accc2014/media/Store/documents/Proceedings-of-ACCC2014.pdf [Accessed June 29, 2016].

Čábyová, L. & Ptačin, J., 2014. Benchmarking comparison of marketing communication of Universities in Slovakia. *Communication Today.*, Vol. 5(1). [Online] Available at: http://www.communicationtoday.sk/benchmarking-comparison-of-marketing-communication-of-universities-in-slovakia/ [Accessed June 2, 2016].

Çankaya, I.H., Döş, I. & Tan, Ç., 2011. Effect of cyber bullying on the distrust levels of pre-service teachers: Internet addiction as mediating variable. *New Educational Review*, Vol. 25(3), pp.53–65. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S1877042810024833 [Accessed June 7, 2016].

Chadwick, A.E., 2014. Toward a Theory of Persuasive Hope: Effects of Cognitive Appraisals, Hope Appeals, and Hope in the Context of Climate Change. *Health communication*, Vol. 236(November), pp.1–14. [Online] Available at: http://www.ncbi.nlm.nih.gov/pubmed/25297455 [Accessed July 1, 2016].

Chapleo, C., 2010. What defines ‘successful’ university brands? *International Journal of Public Sector Management.*, Vol. 23(2), pp.169–183. [Online] Available at: http://eprints.bournemouth.ac.uk/18857/6/licence.txt [Accessed March 14, 2015].

Charry, K.M. & Demoulin, N.T.M., 2012. Behavioural evidence for the effectiveness of threat appeals in the promotion of healthy food to children. *International Journal of Advertising*, Vol. 31(4), pp.773–794. [Online] Available at:

http://www.tandfonline.com/doi/abs/10.2501/IJA-31-4-773-794 [Accessed July 1, 2016].

Chen, Y.T. & Wang, J.H., 2016. Analyzing with Posner's Conceptual Change Model and Toulmin's Model of Argumentative Demonstration in senior high school students' mathematic learning. *International Journal of Information and Education Technology.*, Vol. 6(6), pp.457–464. [Online] Available at: http://www.ijiet.org/vol6/732-M04.pdf [Accessed April 9, 2016].

Choo, K.K.R., 2011. The cyber threat landscape: Challenges and future research directions. *Computers and Security*, Vol. 30(8), pp.719–731. [Online] Available at: http://dx.doi.org/10.1016/j.cose.2011.08.004 [Accessed July 6, 2015].

Choucri, N., Madnick, S. & Ferwerda, J., 2013. Institutional Foundations for Cyber Security: Current Responses and New Challenges. *Information Technology for Development*, Vol. 20(2), pp.96–121. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/02681102.2013.836699 [Accessed June 29, 2016].

Choucri, N., Madnick, S. & Ferwerda, J., 2014. Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*, Vol. 20(2), pp.96–121. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/02681102.2013.836699 [Accessed June 29, 2016].

Chung, J.Y., Lee, J. & Heath, R.L., 2013. Public relations aspects of brand attitudes and customer activity. *Public Relations Review*, Vol. 39(5), pp.432–439. [Online] Available at: http://dx.doi.org/10.1016/j.pubrev.2013.05.001.

Ciftci, N.P. & Delialioglu, O., 2015. Supporting students' knowledge and skills in information technology security through a security portal. *Information Development*, pp.1–11. [Online] Available at: http://idv.sagepub.com/cgi/doi/10.1177/0266666915601463 [Accessed June 29, 2016].

Clark, J.K., Wegener, D.T., Sawicki, V., Petty, R.E. & Briñol, P., 2013. Evaluating the message or the messenger? Implications for self-validation in persuasion. *Personality & social psychology bulletin*, Vol. 39(12), pp.1571–84. [Online] Available at: http://www.ncbi.nlm.nih.gov/pubmed/23969619 [Accessed July 1, 2016].

Clarke, B.D., 2013. *Parents' perceptions and awareness of cyberbullying of children and adolescents.* [Online] Available at: http://ovidsp.ovid.com/ovidweb.cgi?T=JS&CSC=Y&NEWS=N&PAGE=fulltext&D=psyc12&AN=2015-99240-425 [Accessed June 28, 2015].

Clemons, E.K. & Wilson, J., 2015. Students' and parents' attitudes towards online privacy: An international study. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. pp. 4844–4853. [Online] Available at: ieeexplore.ieee.org/iel7/7068092/7069647/07070395.pdf [Accessed June 29, 2016].

Collegiate High School Governing Body., 2016. *Information Systems and Social Media Policy.*, [Online] Available at: http://www.collegiatehigh.co.za/page/information-systems-and-social-media-policy [Accessed September 14, 2016].

Collins, K. & Millard, M., 2013. Transforming education in South Africa: comparative perceptions of a South African social work learning experience. *Educational Review*, Vol. 65(1), pp.70–84.

Commonsense, 2016. Digital citizenship poster. [Online] Available at: https://www.commonsensemedia.org/educators/elementary_poster [Accessed July 3, 2016].

Cornelissen, J., 2014. *Corporate Communication. A guide to theory and practice.* Fourth., SAGE.

Cortes, D., Santamaria, J. & Vargas, J.F., 2013. *Income shocks and crime: evidence from the break down of ponzi schemes .*, [Online] Available at: http://repository.urosario.edu.co/bitstream/handle/10336/11880/dt185.pdf?sequence=3&isAllowed=y [Accessed September 2, 2016].

Creswell, J.W., 2013. *Qualitative inquiry & Research Design. Choosing among five approaches.* Third., USA:SAGE.

Crompton, B., Thompson, D. & Reyes, M., 2016. *Cybersecurity awareness Shrewsbury public schools.*, [Online] Available at: http://commons.clarku.edu/cgi/viewcontent.cgi?article=1001&context=sps_masters_papers [Accessed July 1, 2016].

Cronjé, F. & Van Wyk, J., 2013. Measuring corporate personality with social responsibility benchmarks. *Journal of Global Responsibility*, Vol. 4(2), pp.188–243. [Online] Available at: http://www.emeraldinsight.com/10.1108/JGR-03-2012-0010 [Accessed June 2, 2015].

Dael, N., Perseguers, M.-N., Marchand, C., Antonietti, J.-P. & Mohr, C., 2015. Put on that colour, it fits your emotion: Colour appropriateness as a function of expressed emotion. *Quarterly journal of experimental psychology (2006)*, Vol. 218(July), pp.1–12. [Online] Available at: http://www.ncbi.nlm.nih.gov/pubmed/26339950 [Accessed July 1, 2016].

Dalvit, L., Kromberg, S. & Miya, M., 2014. The data divide in a South African rural community : A survey of mobile phone use in Keiskammahoek. In *Proceedings of the e-Skills for Knowledge Production and Innovation Conference*. pp. 87–100. [Online] Available at: http://proceedings.e-skillsconference.org/2014/e-skills087-100Dalvit842.pdf [Accessed August 7, 2016].

Daramola, D., 2015. Young Children as Internet Users and Parents Perspectives. , pp.1–51. [Online] Available at: jultika.oulu.fi/files/nbnfioulu-201505261650.pdf [Accessed June 28, 2016].

Dasgupta, M., 2015. Exploring the Relevance of Case Study Research. *Vision: The Journal of Business Perspective*, Vol. 19(2), pp.147–160. [Online] Available at: http://vis.sagepub.com/content/19/2/147.abstract [Accessed June 2, 2016].

Davis, J.T., 2012. Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing*, Vol. 35(2), pp.272–284. [Online] Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84861820007&partnerID=40&md5=819a94db50c93820645a8baf3489446d [Accessed June 7, 2016].

Davis, K., Randall, D.P., Ambrose, A. & Orand, M., 2015. ‘I was bullied too’: stories of bullying and coping in an online community. *Information, Communication & Society*, Vol. 18(4), pp.357–375. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/1369118X.2014.952657 [Accessed June 28, 2016].

Deibert, R., 2012. The growing dark side of cyberspace (... and what to do about it). *Penn State Journal of Law & International Affairs*, Vol. 1(2), pp.260–274. [Online]

Available at: http://elibrary.law.psu.edu/jlia/voll/iss2/3 [Accessed June 28, 2016].

De Kadt, J., Norris, S.A., Fleisch, B., Richter, L. & Alvanides, S., 2014. Children's daily travel to school in Johannesburg-Soweto, South Africa: geography and school choice in the Birth to Twenty cohort study. *Children's Geographies*, Vol. 12(2), pp.170–188. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/14733285.2013.812304 [Accessed August 7, 2016].

De Massis, A. & Kotlar, J., 2014. The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy*, Vol. 5(1), pp.15–29. [Online] Available at: http://dx.doi.org/10.1016/j.jfbs.2014.01.007.

Department of Basic Education, 2014. *Report on the Annual National Assessment of 2014. Grades 1 to 6 & 9.*, [Online] Available at: http://www.education.gov.za/Portals/0/Documents/Reports/2014 ANA Dignostic Report Foundation Phase.pdf?ver=2015-02-11-114944-697 [Accessed August 21, 2016].

De Sá Ibraim, S. & Justi, R., 2016. Teachers ' knowledge in argumentation : contributions from an explicit teaching in an initial teacher education programme. *International Journal of Science Education.*, (August), pp.1–30. [Online] Available at: http://dx.doi.org/10.1080/09500693.2016.1221546 [Accessed September 2, 2016].

Desai, Z., 2016. Learning through the medium of English in multilingual South Africa: enabling or disabling learners from low income contexts? *Comparative Education*, Vol. 52(3), pp.343–358. [Online] Available at: http://www.tandfonline.com/doi/full/10.1080/03050068.2016.1185259 [Accessed August 21, 2016].

Devine, P. & Lloyd, K., 2012. Internet use and psychological well-being among 10-year-old and 11-year-old children. *Child Care in Practice*, Vol. 18(1), pp.5–22. [Online] Available at: www.tandfonline.com/doi/abs/10.1080/13575279.2011.621888 [Accessed June 29, 2016].

Deylami, M.H., Mohaghegh, M., Sarrafzadeh, A., McCauley, M., Ardekani, I.T. & Kingston, T., 2015. Capture the talent: secondary school education wtih cyber security competitions. *International Journal in Foundations of Computer Science & Technology (IJFCST).*, Vol. 5(6), pp.55–66. [Online] Available at: wireilla.com/papers/ijfcst/V5N6/5615ijfcst06.pdf [Accessed June 29, 2016].

Diga, K., Nwaiwu, F. & Plantinga, P., 2013. ICT policy and poverty reduction in Africa. *Info*, Vol. 15(5), pp.114–127. [Online] Available at: http://0-www.emeraldinsight.com.innopac.up.ac.za/journals.htm?issn=1463-6697&volume=15&issue=5&articleid=17094563&show=html.

Dimitrova, N., 2013. It Takes More Than Mean End Differentiation to Intentionally Communicate in Infancy . A Semiotic Perspective on Early Communication. *Cultural-Historical Psychology*, Vol. 3, pp.81–90. [Online] Available at: http://psyjournals.ru/en/kip/2013/n3/63014.shtml [Accessed September 14, 2016].

Dlamini, Z. & Modise, M., 2012. Cyber security awareness initiatives in South Africa: a synergy aproach. In *7th International Conference on Information Warfare and Security*. pp. 1–10. [Online] Available at: http://hdl.handle.net/10204/5941 [Accessed February 27, 2016].

Domigan, J., Glassman, T. & Miller, J., 2015. Message testing to create effective health communication campaigns. *Health Education*, Vol. 115(5), pp.480–494. [Online] Available at: http://www.emeraldinsight.com/doi/abs/10.1108/HE-02-2014-0012 [Accessed December 28, 2015].

Donaldson, R., Mehlomakhulu, T., Darkey, D., Dyssel, M. & Siyongwana, P., 2013. Relocation: To be or not to be a black diamond in a South African township? *Habitat International*, Vol. 39, pp.114–118. [Online] Available at: http://dx.doi.org/10.1016/j.habitatint.2012.10.018 [Accessed August 9, 2015].

Donohue, D. & Bornman, J., 2014. The challenges of realising inclusive education in South Africa. *South Africa Journal of Education.*, Vol. 34(2), pp.1–14. [Online] Available at: www.scielo.org.za/pdf/saje/v34n2/03.pdf [Accessed August 7, 2016].

Dooley, J.A., Jones, S.C. & Iverson, D., 2012. Web 2.0 an assessment of social marketing principles. *Journal of Social Marketing*, Vol. 2(3), pp.207–221. [Online] Available at: http://www.emeraldinsight.com/doi/abs/10.1108/20426761211265195 [Accessed December 28, 2015].

Dorfman, L., Ervice, J. & Woodruff, K., 2002. *Voices for change: A taxonomy of public communications campaigns and their evaluation challenges.*, [Online] Available at: www.bmsg.org/pdfs/Taxonomy_Evaluation.pdf [Accessed July 3, 2016].

Ekos Research Associates, 2011. *Baseline, online probability survey of Internet users regarding cyber security.*,

Elkins, A.C., Derrick, D.C., Burgoon, J.K. & Nunamaker, J.F., 2011. Predicting users' perceived trust in embodied conversational agents using vocal dynamics. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. pp. 579–588. [Online] Available at: ieeexplore.ieee.org/iel5/6148328/6148595/06148598.pdf [Accessed July 26, 2015].

Elliott, I.A. & Beech, A.R., 2009. Understanding online child pornography use: Applying sexual offense theory to internet offenders. *Aggression and Violent Behavior*, Vol. 14(3), pp.180–193. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S1359178909000305 [Accessed April 7, 2016].

Elo, S., Kääriäinen, M., Kanste, O., Polkki, T., Utriainen, K. & Kyngas, H., 2014. Qualitative Content Analysis: A Focus on Trustworthiness. *SAGE Open*, Vol. 4(1), pp.1–10. [Online] Available at: http://sgo.sagepub.com/lookup/doi/10.1177/2158244014522633.

Engelbrecht, P., Nel, M., Smit, S. & van Deventer, M., 2016. The idealism of education policies and the realities in schools: the implementation of inclusive education in South Africa. *International Journal of Inclusive Education*, Vol. 20(5), pp.520–535. [Online] Available at: https://www.researchgate.net/publication/283788561_The_idealism_of_education_policies_and_the_realities_in_schools_the_implementation_of_inclusive_education_in_South_Africa?enrichId=rgreq-81549d6f-a0f7-473e-b0b0-447e5ecf1606&enrichSource=Y292ZXJQYWdlOzI4M [Accessed August 9, 2016].

Epstein, D., 2014. Race-ing class ladies: lineages of privilege in an elite South African school. *Globalisation, Societies and Education*, Vol. 12(2), pp.244–261. [Online] Available at: http://libsta28.lib.cam.ac.uk:2059/doi/pdf/10.1080/14767724.2014.890887\nhttp://l ibsta28.lib.cam.ac.uk:2059/doi/abs/10.1080/14767724.2014.890887#.VOZXOsYVxQI [Accessed August 21, 2016].

Epure, M., Eisenstat, E. & Dinu, C., 2014. Semiotics and persuasion in marketing communication. *Linguistic & Philosophical Investigations*, Vol. 13, pp.592–605. [Online] Available at: http://ezproxy.taylors.edu.my/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=96159748&site=eds-live&scope=site [Accessed June 13, 2016].

Estanyol, E., 2012. Marketing, public relations, and how Web 2.0 is changing their relationship: A qualitative assessment of PR consultancies operating in Spain. *Public Relations Review*, Vol. 38(5), pp.831–837. [Online] Available at: http://linkinghub.elsevier.com/retrieve/pii/S0363811112000707 [Accessed February 3, 2014].

Evans-Lacko, S., London, J., Little, K., Henderson, C. & Thornicroft, G., 2010. Evaluation of a brief anti-stigma campaign in Cambridge: do short-term campaigns work? *BMC Public Health*, Vol. 10(339), pp.1–6. [Online] Available at: http://www.biomedcentral.com/1471-2458/10/339 [Accessed July 6, 2016].

Ewing, M.T., 2009. Integrated marketing communications measurement and evaluation. *Journal of Marketing Communications*, Vol. 15(2–3), pp.103–117. [Online] Available at: http://dx.doi.org/10.1080/13527260902757514 [Accessed June 29, 2016].

Ey, L. & Cupit, C.G., 2011. Exploring young childrens understanding of risks associated with Internet usage and their concepts of management strategies. *Journal of Early Childhood Research*, Vol. 9(1), pp.53–65. [Online] Available at: http://ecr.sagepub.com/cgi/doi/10.1177/1476718X10367471\nhttp://ecr.sagepub.com/content/9/1/53.short [Accessed June 2, 2015].

Fassin, Y., 2011. A dynamic perspective in Freeman's Stakeholder Model. *Journal of Business Ethics*, Vol. 96(July), pp.39–49. [Online] Available at: link.springer.com/article/10.1007/s10551-011-0942-6 [Accessed July 3, 2015].

Felt, L.J. & Vartabedian, V., 2012. Explore locally , excel digitally : A participatory learning after-school program for enriching citizenship on- and offline. *The Journal of Media Literacy Education*, Vol. 4(3), pp.213–228. [Online] Available at:

digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1103&context=jmle [Accessed July 2, 2016].

Feng, Y. & Xie, W., 2014. Teens’ concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior*, Vol. 33, pp.153–162. [Online] Available at: http://dx.doi.org/10.1016/j.chb.2014.01.009 [Accessed June 29, 2016].

Ferguson, G. & Phau, I., 2013. Adolescent and young adult response to fear appeals in anti-smoking messages. *Young Consumers*, Vol. 14(2), pp.155–166. [Online] Available at: http://www.emeraldinsight.com/10.1108/17473611311325555 [Accessed June 2, 2015].

Fisher, H.D., Magee, S. & Mohammed-Baksh, S., 2015. Do they care? An experiment exploring millennials’ perception of source credibility in radio broadcast news. *Journal of Radio & Audio Media*, Vol. 22(2), pp.304–324. [Online] Available at: http://www.tandfonline.com/doi/full/10.1080/19376529.2015.1083154 [Accessed July 1, 2016].

Flyvbjerg, B., 2006. Five misunderstandings about case-study research. *Qualitative Inquiry*, Vol. 12(2), pp.219–245. [Online] Available at: flyvbjerg.plan.aau.dk/Publications2006/0604FIVEMISPUBL2006.pdf [Accessed June 2, 2015].

Fourie, L., Sarrafzadeh, A., Pang, S., Kingston, T. & Watters, P., 2014. The global cyber security workforce - An ongoing human capital crisis. In *2014 Global Business and Technology Association Conference*. Global Business and Technology Association, pp. 173–184. [Online] Available at: unitec.researchbank.ac.nz/bitstream/10652/2457/1/Cyber2.pdf [Accessed June 29, 2016].

Fox, J. & Tang, W.Y., 2014. Sexism in online video games: The role of conformity to masculine norms and social dominance orientation. *Computers in Human Behavior*, Vol. 33, pp.314–320. [Online] Available at: http://dx.doi.org/10.1016/j.chb.2013.07.014 [Accessed June 28, 2016].

Fraustino, J.D. & Ma, L., 2015. CDC’s use of social media and humor in a risk campaign—‘Preparedness 101: Zombie Apocalypse’. *Journal of Applied*

Communication Research, Vol. 43(2), pp.222–241. [Online] Available at: http://dx.doi.org/10.1080/00909882.2015.1019544\nhttp://www.tandfonline.com/doi/pdf/10.1080/00909882.2015.1019544\nhttp://www.tandfonline.com/doi/full/10.1080/00909882.2015.1019544 [Accessed June 25, 2016].

Frededay, J. & Muir-Cochrane, E., 2006. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods.*, Vol. 5(1). [Online] Available at: https://sites.ualberta.ca/~iiqm/backissues/5_1/HTML/fereday.htm [Accessed February 27, 2016].

Freeman, R.E., Harrison, J.S., Wicks, A.C., Parmar, B.L. & Colle, S. de, 2010. Stakeholder Theory: The state of the art. *The Academy of Management Annals.*, Vol. 4(1), pp.403–445. [Online] Available at: https://www.researchgate.net/publication/235458104_Stakeholder_Theory_The_State_of_the_Art [Accessed July 3, 2016].

Furman, S., Theofanos, M.F., Choong, Y.Y. & Stanton, B., 2012. Basing cybersecurity training on user perceptions. *IEEE Security and Privacy*, Vol. 10(2), pp.40–49. [Online] Available at: ieeexplore.ieee.org/document/6112743/ [Accessed July 5, 2015].

Furnell, S. & Moore, L., 2014. Security literacy: The missing link in today's online society? *Computer Fraud and Security*, (5), pp.12–18. [Online] Available at: http://dx.doi.org/10.1016/S1361-3723(14)70491-9 [Accessed June 27, 2016].

Futcher, L., Schroder, C. & von Solms, R., 2010. Information security education in South Africa. *Information Management & Computer Security*, Vol. 18, pp.366–374. [Online] Available at: www.emeraldinsight.com/doi/abs/10.1108/09685221011095272 [Accessed June 3, 2016].

Gamreklidze, E., 2014. Cyber security in developing countries, a digital divide issue. *Journal of International Communication*, Vol. 20(2), pp.200–217. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/13216597.2014.954593\nhttp://nca.tandfonline.com/doi/abs/10.1080/13216597.2014.954593#.VBHXzmMZnS0\nhttp://nca.tandfonline.com/doi/abs/10.1080/13216597.2014.954593?journalCode=rico2

0#.VIjtVHtuPyA [Accessed June 13, 2016].

Gcaza, N., Von Solms, R. & Van Vuuren, J., 2015. An ontology for a national cyber-security culture environment. In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA).* pp. 1–10. [Online] Available at: https://www.cscan.org/openaccess/?id=253 [Accessed June 23, 2016].

Gerson, I., 2013. *Investigating the effectiveness of a ‘ Surfing Safely ’ school educational initiative in increasing the awareness of vulnerable children with regards to Internet safety and risks in a Jewish community school.* [Online] Available at: https://ujdigispace.uj.ac.za [Accessed June 14, 2016].

Giannakas, F., Kambourakis, G. & Gritzalis, S., 2015. CyberAware: A mobile game-based app for cybersecurity education and awareness. *2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)*, (November), pp.54–58. [Online] Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84962385368&partnerID=tZOtx3y1 [Accessed February 18, 2016].

Gibbert, M. & Ruigrok, W., 2010. The what’’ and how’’ of case study rigor: three strategies based on published work. *Organizational Research Methods*, Vol. 13(4), pp.710–737. [Online] Available at: orm.sagepub.com/content/13/4/710.abstract [Accessed February 18, 2016].

Goh, W.., Bay, S. & Chen, V.H., 2015. Young school children’s use of digital devices and parental rules. *Telematics and Informatics*, Vol. 32(4), pp.787–795. [Online] Available at: http://dx.doi.org/10.1016/j.tele.2015.04.002 [Accessed June 3, 2016].

Goi, C.L., 2009. A review of marketing mix: 4Ps or more? *International Journal of Marketing Studies*, Vol. 1(1), pp.2–15. [Online] Available at: www.ccsenet.org/journal/index.php/ijms/article/download/97/1552 [Accessed June 9, 2015].

Goode, L., 2010. Cultural citizenship online: the Internet and digital culture. *Citizenship Studies*, Vol. 14(5), pp.527–542. [Online] Available at: www.tandfonline.com/doi/abs/10.1080/13621025.2010.506707 [Accessed July 6, 2016].

Görzig, A. & Ólafsson, K., 2013. What makes a bully a cyberbully? Unravelling the characteristics of cyberbullies across twenty-five European countries. *Journal of Children and Media*, Vol. 7(1), pp.9–27. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/17482798.2012.739756 [Accessed June 6, 2016].

Government of South Africa, 2016. South African Department of Basic Education. [Online] Available at: http://www.education.gov.za/ [Accessed August 21, 2016].

Grbich, C., 2013. *Qualitative Data Analysis. An introduction.*, UK: SAGE.

Greenberg, G.A. & Sze, H.Y., 2010. *Ponzi schemes and bank liability: the new 'red flags,' the risks and the decision whether to terminate the customer relationship*, [Online] Available at: files.mwe.com/info/pubs/FFLR_0110.pdf [Accessed June 29, 2016].

Gregory, A., 2010. *Planning and Managing Public Relations Campaigns. A Strategic Approach.* Third., Kogan Page Limited.

Gregory, S. & Masters, Y., 2012. Real thinking with virtual hats: A role-playing activity for pre-service teachers in Second Life. *Australasian Journal of Educational Technology*, Vol. 28(3), pp.420–440. [Online] Available at: https://ajet.org.au/index.php/AJET/article/viewFile/843/138 [Accessed July 3, 2015].

Grobler, M., Dlamini, Z., Ngobeni, S. & Labuschagne, A., 2011. Towards a cyber security aware rural community. In *Proceedings of the 2011 Information Security for South Africa (ISSA) Conference.* pp. 1–7. [Online] Available at: http://goo.gl/680YtV [Accessed June 7, 2016].

Grobler, M., Jansen van Vuuren, J. & Zaaiman, J., 2011. Evaluating cyber security awareness in South Africa. *10th European Conference on Warfare and Security*, (June 2016), pp.125–133. [Online] Available at: researchspace.csir.co.za/dspace/bitstream/10204/5108/1/Grobler1_2011.pdf? [Accessed June 7, 2016].

Groeger, L. & Buttle, F., 2014. Word-of-mouth marketing. *European Journal of Marketing*, Vol. 48(7/8), pp.1186–1208. [Online] Available at: http://www.emeraldinsight.com/doi/full/10.1108/EJM-02-2012-0086.

Grouchy, P., D'Eleuterio, G.M.T., Christiansen, M.H. & Lipson, H., 2016. *On The Evolutionary Origin of Symbolic Communication*, Nature Publishing Group. [Online] Available at: http://www.nature.com/articles/srep34615 [Accessed September 21, 2016].

Gudmundsdottir, G.B., 2011. *From digital divide to digital opportunities? A critical perspective on the digital divide in South African schools*. [Online] Available at: https://www.duo.uio.no/handle/10852/52519 [Accessed August 21, 2016].

Gumbo, S., Jere, N. & Terzoli, A., 2012. A qualitative analysis to determine the readiness of rural communities to adopt ICTs: a Siyakhula Living Lab case study. In *IST Africa Conference Proceedings*. pp. 1–9. [Online] Available at: http://siyakhulall.org/sites/default/files/ISTAfrica_Paper_ref_89_doc_4818.pdf [Accessed August 20, 2016].

Gurnani, R., Pandey, K. & Rai, S.K., 2014. A scalable model for implementing cyber security exercises. *2014 International Conference on Computing for Sustainable Global Development, INDIACom*, pp.680–684. [Online] Available at: ieeexplore.ieee.org/iel7/6821332/6827395/06828048.pdf [Accessed June 29, 2016].

Guttman, N., 2015. Persuasive appeals in road safety communication campaigns: Theoretical frameworks and practical implications from the analysis of a decade of road safety campaign materials. *Accident Analysis and Prevention*, Vol. 84, pp.153–164. [Online] Available at: http://dx.doi.org/10.1016/j.aap.2015.07.017 [Accessed June 3, 2016].

Halliburton, C., 2012. An integrative framework of corporate brand equity. *EuroMed Journal of Business*, Vol. 7(3), pp.243–255. [Online] Available at: http://dx.doi.org/10.1108/14502191211265307\nDownloaded.

Hamade, S.N., 2015. Parental awareness and mediation of children's Internet use in Kuwait. In *2015 12th International Conference on Information Technology - New Generations*. pp. 640–645. [Online] Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7113546 [Accessed June 26, 2016].

Hammick, J.K. & Lee, M.J., 2014. Do shy people feel less communication apprehension online? the effects of virtual reality on the relationship between personality characteristics and communication outcomes. *Computers in Human Behavior*, Vol. 33, pp.302–310. [Online] Available at: http://dx.doi.org/10.1016/j.chb.2013.01.046.

Hamzah, Z.L., Syed Alwi, S.F. & Othman, M.N., 2014. Designing corporate brand experience in an online context: A qualitative insight. *Journal of Business Research*, Vol. 67(11), pp.2299–2310. [Online] Available at: http://dx.doi.org/10.1016/j.jbusres.2014.06.018 [Accessed February 25, 2015].

Hanafy, I.M. & Sanad, R., 2015. Colour preferences according to educational background. *Procedia - Social and Behavioral Sciences*, Vol. 205(May), pp.437–444. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S1877042815050521 [Accessed July 1, 2016].

Hansche, S., 2001. Designing a security awareness program: part I. *Information Systems Security*, Vol. 9(6), p.14. [Online] Available at: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=3943159&site=eds-live [Accessed June 13, 2015].

Harrison, T.R., 2014. Enhancing Communication Interventions and Evaluations through Communication Design. *Journal of Applied Communication Research*, Vol. 42(2), pp.135–149. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/00909882.2013.825047 [Accessed June 26, 2016].

Hashemnezhad, H., 2015. Qualitative content analysis research: a review article. *Journal of ELT and Applied Linguistics (JELTSL)*, Vol. 3(1), pp.54–62. [Online] Available at: http://slideshowes.com/doc/1586293/qualitative-content-analysis-research--a-review-article [Accessed June 13, 2016].

Hector’s World Limited, Hector’s World. [Online] Available at: http://hectorsworld.netsafe.org.nz/ [Accessed June 26, 2016].

Henley, N., Raffin, S. & Caemmerer, B., 2011. The application of marketing principles to a social marketing campaign. *Marketing Intelligence & Planning*, Vol. 29, pp.697–706. [Online] Available at: www.emeraldinsight.com/doi/abs/10.1108/02634501111178712 [Accessed June 2, 2016].

Henshel, D., Cains, M.G., Hoffman, B. & Kelley, T., 2015. Trust as a Human Factor in Holistic Cyber Security Risk Assessment. *Procedia Manufacturing*, Vol. 3(Ahfe), pp.1117–1124. [Online] Available at: http://linkinghub.elsevier.com/retrieve/pii/S2351978915001870 [Accessed June 7, 2016].

Heyd-Metzuyanim, E. & Graven, M., 2016. Between people-pleasing and mathematizing: South African learners' struggle for numeracy. *Educational Studies in Mathematics*, Vol. 91(3), pp.349–373. [Online] Available at: link.springer.com/article/10.1007/s10649-015-9637-8 [Accessed August 21, 2016].

Hill, L.D., 2014. Race, school choice and transfers to opportunity: implications for educational stratification in South Africa. *British Journal of Sociology of Education*, Vol. 5692(August), pp.1–28. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/01425692.2014.952810 [Accessed August 9, 2016].

Hill, V., 2015. Digital citizenship through game design in Minecraft. *New Library World*, Vol. 116(7/8), pp.369–382. [Online] Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84931098584&partnerID=tZOtx3y1 [Accessed July 1, 2016].

Hlatshwayo, M. & Vally, S., 2014. Violence, resilience and solidarity: The right to education for child migrants in South Africa. *School Psychology International*, Vol. 35(3), pp.266–279. [Online] Available at: spi.sagepub.com/content/35/3/266.short [Accessed August 9, 2016].

Hollensen, S. & Schimmelpfennig, C., 2013. Selection of celebrity endorsers: A case approach to developing an endorser selection process model. *Marketing Intelligence & Planning*, Vol. 31(1), pp.88–102. [Online] Available at: http://www.emeraldinsight.com/journals.htm?articleid=17076796&show=abstract\nhttp://www.emeraldinsight.com/journals.htm?issn=0263-4503&volume=31&issue=1&articleid=17076796&show=html [Accessed August 9, 2016].

Hope, A., 2015. Schoolchildren, governmentality and national e-safety policy discourse. *Discourse-Studies in the Cultural Politics of Education*, Vol. 36(June), pp.343–353. [Online] Available at: www.tandfonline.com/doi/pdf/10.1080/01596306.2013.871237 [Accessed June 28, 2016].

Hosany, S., Prayag, G., Martin, D. & Lee, W.-Y., 2013. Theory and strategies of anthropomorphic brand characters from Peter Rabbit, Mickey Mouse, and Ronald McDonald, to Hello Kitty. *Journal of Marketing*, Vol. 29(1–2), pp.48–68. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/0267257X.2013.764346 [Accessed July 3, 2016].

Houghton, C., Casey, D., Shaw, D. & Murphy, K., 2013. Rigour in qualitative case-study research. *Nurse Researcher*, Vol. 20(4), pp.12–17. [Online] Available at: https://www.ncbi.nlm.nih.gov/pubmed/23520707 [Accessed August 21, 2016].

Howitt, M. & McManus, J., 2012. Stakeholder Management: An instrument for decision making. *Management Services*, Vol. 56(3), pp.29–34. [Online] Available at: http://search.proquest.com.ezp.waldenulibrary.org/abicomplete/docview/1419016056/13FFF4E9C25629C3D00/5?accountid=14872\nhttp://media.proquest.com.ezp.waldenulibrary.org/media/pq/classic/doc/3041149131/fmt/pi/rep/NONE?hl=&cit:auth=Howitt,+Michael;McM [Accessed June 23, 2015].

Hughes, D.R., 2016. Hillary Clinton Promises to Protect Children from Sexual Exploitation Online. *Enough Is Enough*. [Online] Available at: http://enough.org/news/2Y1OMKD3W1 [Accessed October 26, 2016].

Hunter, M., 2015. Schooling choice in South Africa: The limits of qualifications and the politics of race, class and symbolic power. *International Journal of Educational Development*, Vol. 43, pp.41–50. [Online] Available at: http://dx.doi.org/10.1016/j.ijedudev.2015.04.004 [Accessed August 9, 2016].

Hussain, Z., Williams, G.A. & Griffiths, M.D., 2015. An exploratory study of the association between online gaming addiction and enjoyment motivations for playing massively multiplayer online role-playing games. *Computers in Human Behavior*, Vol. 50, pp.221–230. [Online] Available at: http://dx.doi.org/10.1016/j.chb.2015.03.075 [Accessed June 28, 2015].

Ibraim, S.D.S., Justi, R., De Sá Ibraim, S. & Justi, R., 2016. Teachers ' knowledge in argumentation : contributions from an explicit teaching in an initial teacher education programme. *International Journal of Science Education.*, Vol.

693(August), pp.1–30. [Online] Available at: www.tandfonline.com/doi/full/10.1080/09500693.2016.1221546 [Accessed June 2, 2015].

Idris, M.Z. & Whitfield, T.W. a, 2014. Swayed by the logo and name: Does university branding work? *Journal of Marketing for Higher Education*, Vol. 24(1), pp.41–58. [Online] Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84903522688&partnerID=40&md5=085a18ff361889e173f7cf9f89da53f1 [Accessed April 9, 2015].

Illia, L., 2012. Corporate communication and corporate marketing: Their nature, histories, differences and similarities. *Corporate Communications: An International Journal*, Vol. 17(4), pp.415–433. [Online] Available at: https://www.econbiz.de/Record/corporate-communication-and-corporate-marketing-their-nature-histories-differences-and-similarities-illia-laura/10009671833 [Accessed April 9, 2015].

Isman, A. & Gungoren, O.C., 2013. Being digital citizen. In *4th International Conference on New Horizons in Education.* Procedia - Social and Behavioral Sciences, pp. 551–556. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S1877042813046788 [Accessed June 9, 2015].

Israelashvili, M., Kim, T. & Bukobza, G., 2012. Adolescents' over-use of the cyber world – Internet addiction or identity exploration? *Journal of Adolescence*, Vol. 35(2), pp.417–424. [Online] Available at: https://www.ncbi.nlm.nih.gov/pubmed/21803411 [Accessed June 7, 2016].

James, K.J., Albrecht, J.A., Litchfield, R.E. & Weishaar, C.A., 2013. A summative evaluation of a food safety social marketing campaign '4-Day Throw-Away' using traditional and social media. *Journal of Food Science Education*, Vol. 12(3), pp.48–55. [Online] Available at: onlinelibrary.wiley.com/doi/10.1111/1541-4329.12010/abstract [Accessed June 26, 2016].

James, M., 2011. Ready, aim, fire: key messages in public relations campaigns. *PRISM Journal*, Vol. 8(8 (1)), pp.1–18. [Online] Available at: www.prismjournal.org/fileadmin/8_1/James.pdf [Accessed June 16, 2014].

Jansen Van Vuuren, J., Phahlamohlaka, J. & Brazzoli, M., 2010. The impact of the increase in broadband access on South African national security and the average citizen. *Journal of Information Warfare.*, Vol. 9(3), pp.171–181. [Online] Available at: https://www.jinfowar.com/journal/volume-9-issue-3/impact-increase-broadband-access-south-african-national-security-average-citizen [Accessed June 28, 2016].

Jarvis, J.W., Rhodes, R.E., Deshpande, S., Berry, T.R., Chulak-Bozzer, T., Faulkner, G., Spence, J.C., Tremblay, M.S. & Latimer-Cheung, A.E., 2014. Investigating the role of brand equity in predicting the relationship between message exposure and parental support for their child’s physical activity. *Social Marketing Quarterly*, Vol. 20(2), pp.103–115. [Online] Available at: smq.sagepub.com/content/early/2014/03/18/1524500414528183 [Accessed June 2, 2016].

Jiang, Q. & Leung, L., 2012. Effects of individual differences, awareness-knowledge, and acceptance of Internet addiction as a health risk on willingness to change internet habits. *Social Science Computer Review*, Vol. 30(2), pp.170–183. [Online] Available at: ssc.sagepub.com/content/30/2/170.abstract [Accessed June 28, 2015].

Jobi, T.G. & Kritzinger, E., 2014. Online Awareness among Sepedi School Children in South Africa. In *Proceedings of the Ireland International Conference on Education (IICE-2014).* pp. 337–341.

Johansen, T.S. & Andersen, S.E., 2012. Co-creating ONE: rethinking integration within communication. *Corporate Communications: An International Journal*, Vol. 17(3), pp.272–288. [Online] Available at: www.emeraldinsight.com/doi/pdf/10.1108/13563281211253520 [Accessed June 2, 2015].

Johnson, L.D. & Branson, R.A., 2012. Counselors ’ guidelines for the healthy development of youth in the digital age. *Ideas and Research You Can Use: VISTAS*, Vol. 1, pp.1–7. [Online] Available at: https://www.counseling.org/resources/library/vistas/vistas12/Article_40.pdf [Accessed February 25, 2016].

Johnson, M., 2014. *Cybercrime: Threats and Solutions*, [Online] Available at: http://www.finanstilsynet.no/Global/Temasider/IT-tilsyn/Cybercrime-Threats-and-

Solutions-Sample1.pdf [Accessed June 26, 2016].

Johnston, A.., Warkentin, M. & Siponen, M., 2013. A Conceptual Framework for Understanding the Effects of Corporate Social Marketing on Consumer Behavior. *Journal of Marketing Management*, Vol. 39(1), pp.113–134. [Online] Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84914100509&partnerID=40&md5=204210939394c814ade8285beb8bc151.

Johnston, A.C., Warketin, M. & Siponen, M., 2015. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, Vol. 39(1), pp.113–134. [Online] Available at: https://www.researchgate.net/publication/271328235_An_Enhanced_Fear_Appeal_Rhetorical_Framework_Leveraging_Threats_to_the_Human_Asset_through_Sanctioning_Rhetoric [Accessed July 1, 2016].

Jones, L.M. & Mitchell, K.J., 2015. Defining and measuring youth digital citizenship. *New Media & Society*, pp.1–17. [Online] Available at: http://nms.sagepub.com/content/early/2015/03/24/1461444815577797\nhttp://nms.sagepub.com.gate2.library.lse.ac.uk/content/early/2015/03/24/1461444815577797.abstract?rss=1\nhttp://nms.sagepub.com.gate2.library.lse.ac.uk/content/early/2015/03/24/146144481557 [Accessed July 1, 2016].

Jones, L.M., Mitchell, K.J. & Walsh, W.A., 2012. *Evaluation of Internet child safety materials used by ICAC task forces in school and community settings*, [Online] Available at: https://www.ncjrs.gov/pdffiles1/nij/grants/242016.pdf [Accessed July 1, 2016].

Julisch, K., 2013. Understanding and overcoming cyber security anti-patterns. *Computer Networks*, Vol. 57(10), pp.2206–2211. [Online] Available at: http://dx.doi.org/10.1016/j.comnet.2012.11.023 [Accessed June 7, 2016].

Juszczyk, S., 2014. Ethnography of virtual phenomena and processes on the Internet. *The New Educational Review*, Vol. 35(2), pp.206–216. [Online] Available at: www.educationalrev.us.edu.pl/e36/a16.pdf [Accessed June 28, 2016].

Kajzer, M., Darcy, J., Crowell, C.R., Striegel, A. & Van Bruggen, D., 2014. An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers and Security*, Vol. 43, pp.64–76. [Online] Available at: http://dx.doi.org/10.1016/j.cose.2014.03.003 [Accessed June 3, 2016].

Kalaitzaki, A.E. & Birtchnell, J., 2014. The impact of early parenting bonding on young adults' Internet addiction, through the mediation effects of negative relating to others and sadness. *Addictive Behaviors*, Vol. 39(3), pp.733–736. [Online] Available at: http://dx.doi.org/10.1016/j.addbeh.2013.12.002 [Accessed June 28, 2016].

Kane, M.T., 2013. Validating the interpretations and uses of test scores. *Journal of Educational Measurement*, Vol. 50(1), pp.1–73. [Online] Available at: onlinelibrary.wiley.com/doi/10.1111/jedm.12000/abstract [Accessed June 29, 2016].

Kapoulas, A., 2012. Understanding challenges of qualitative research: rhetorical issues and reality traps. *Qualitative Market Research: An International Journal*, Vol. 15(4), pp.354–368. [Online] Available at: www.emeraldinsight.com/doi/full/10.1108/13522751211257051 [Accessed August 21, 2016].

Kayworth, T. & Whitten, D., 2010. Effective information security requires a balance of social and technology factors. *MIS Quarterly ExecutiveQuarterly Executive*, Vol. 9(3), pp.163–175. [Online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2058035 [Accessed June 27, 2015].

Kemp, E., Kennett-Hensel, P. a. & Kees, J., 2013. Pulling on the Heartstrings: Examining the Effects of Emotions and Gender in Persuasive Appeals. *Journal of Advertising*, Vol. 42(1), pp.69–79. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/00913367.2012.749084 [Accessed July 1, 2016].

Kennison, P. & Read, M., 2003. The internet and child protection (Part 1). *Safer Communities*, Vol. 2(2), pp.20–25. [Online] Available at: www.emeraldinsight.com/doi/pdf/10.1108/17578043200300014 [Accessed June 2, 2016].

Khurana, A., Bleakley, A., Jordan, A.B. & Romer, D., 2015. The protective effects of parental monitoring and Internet restriction on adolescents' risk of online harassment. *Journal of Youth and Adolescence*, Vol. 44(5), pp.1039–1047.

[Online] Available at: https://www.ncbi.nlm.nih.gov/pubmed/25504217 [Accessed June 28, 2016].

Kim, E.B., 2014. Recommendations for information security awareness training for college students. *Information Management & Computer Security*, Vol. 22(1), pp.115–126. [Online] Available at: http://www.emeraldinsight.com/10.1108/IMCS-01-2013-0005 [Accessed June 2, 2016].

Kim, J.Y. & Kiousis, S., 2012. The role of affect in agenda building for Public Relations: implications for Public Relations outcomes. *Journalism & Mass Communication Quarterly*, Vol. 89(4), pp.657–676. [Online] Available at: jmq.sagepub.com/content/89/4/657.short [Accessed June 2, 2016].

Kim, K. & Kim, K., 2015. Internet game addiction, parental attachment, and parenting of adolescents in South Korea. *Journal of Child & Adolescent Substance Abuse*, Vol. 24(6), pp.366–371. [Online] Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84943363443&partnerID=tZOtx3y1 [Accessed June 13, 2016].

Kivunja, C., 2015. Using De Bono's six thinking hats model to teach critical thinking and problem solving skills essential for success in the 21st century economy. *Creative Education*, Vol. 6(March), pp.380–391. [Online] Available at: www.scirp.org/journal/PaperInformation.aspx?PaperID=54681 [Accessed September 16, 2016].

Kokkinos, C.M., Antoniadou, N., Asdre, A. & Voulgaridou, K., 2016. Parenting and Internet behavior predictors of cyber-bullying and cyber-victimization among preadolescents. *Deviant Behavior*, Vol. 37(4), pp.439–455. [Online] Available at: http://dx.doi.org/10.1080/01639625.2015.1060087 [Accessed June 28, 2016].

Kondyushova, L., 2014. Child protection on the Internet. A teaching framework for Russian schools. , pp.1–117. [Online] Available at: othes.univie.ac.at/32195/1/2014-03-10_1106200.pdf [Accessed June 28, 2016].

Korpela, K., 2015. Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, Vol. 24(1–3), pp.72–77. [Online] Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84937514573&partnerID=tZOtx3y1\nhttp://www.tandfonline.com/doi/full/10.1080/

19393555.2015.1051676 [Accessed June 13, 2016].

Kortjan, N., 2013. *A cyber security awareness and education framework for South Africa*. [Online] Available at: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0CEUQFjAF&url=http://contentpro.seals.ac.za/iii/cpro/app?id=0865119265660214&itemId=1014829&lang=eng&service=blob&suite=def&ei=L6tpVMuILYOrPMLXgdAC&usg=AFQjCNEihfIKD7OdI4JytH67NSl3lSqDTg&s [Accessed February 27, 2016].

Kortjan, N. & Von Solms, R., 2014. A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, Vol. 52, pp.29–41. [Online] Available at: http://connection.ebscohost.com/c/articles/96905714/conceptual-framework-cyber-security-awareness-education-sa [Accessed February 27, 2016].

Kortjan, N., Von Solms, R. & Van Niekerk, J., 2012. Ethical guidelines for cyber-related services aimed at the younger generations. In *Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance.* pp. 205–215. [Online] Available at: https://www.cscan.org/openaccess/?id=33 [Accessed February 27, 2016].

Kotler, P., Armstrong, G. & Tait, M. eds., 2010. *Principles of Marketing. Global and Southern African Perspectives.*, South Africa: Pearson Education Limited.

Kritzinger, E., 2012. Cyber Security Awareness Workbook. [Online] Available at: http://eagle.unisa.ac.za/elmarie/images/Pdf/book.pdf [Accessed December 28, 2015].

Kritzinger, E., 2015. Enhancing cyber safety awareness among school children in South Africa through gaming. In *Proceedings of the 2015 Science and Information Conference, SAI 2015*. pp. 1243–1248. [Online] Available at: http://ieeexplore.ieee.org/iel7/7222825/7237120/07237303.pdf?arnumber=7237303 [Accessed June 7, 2016].

Kritzinger, E., 2014. Online safety in South Africa - a cause for growing concern. *Information Security for South Africa - Proceedings of the ISSA 2014 Conference.*, pp.1–7. [Online] Available at: ieeexplore.ieee.org/document/6950502/ [Accessed June 7, 2016].

Kritzinger, E., 2016. Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal*, Vol. 28 (1)(July), pp.1–17. [Online] Available at: http://sacj.cs.uct.ac.za/index.php/sacj/article/view/369 [Accessed August 22, 2016].

Kritzinger, E. & Padayachee, K., 2013. Engendering an e-safety awareness culture within the South African context. In *IEEE AFRICON Conference*. pp. 1–5. [Online] Available at: ieeexplore.ieee.org/document/6757708/ [Accessed June 20, 2016].

Kritzinger, E. & von Solms, B., 2012. A framework for cyber security in Africa. *Innovation Vision 2020: Sustainable growth, Entrepreneurship, and Economic Development - Proceedings of the 19th International Business Information Management Association Conference.*, Vol. 1, pp.438–447. [Online] Available at: http://www.ibimapublishing.com/journals/JIACS/2012/322399/322399.html [Accessed June 2, 2015].

Kritzinger, E. & Von Solms, S.H., 2010. Cyber security for home users: a new way of protection through awareness enforcement. *Computers and Security*, Vol. 29(8), pp.840–847. [Online] Available at: http://dx.doi.org/10.1016/j.cose.2010.08.001 [Accessed January 1, 2015].

Kropp, E.L., 2015. Using social scientific criteria to evaluate cultural theories: encoding/decoding evaluated. *An International Journal of Pure Communication Inquiry.*, Vol. 3(2), pp.10–26. [Online] Available at: http://komejournal.com/files/KOME_EvanKropp.pdf [Accessed November 29, 2015].

Kshetri, N., 2015. Cybercrime and cybersecurity issues in the BRICS economies. *Journal of Global Information Technology Management*, Vol. 18(4), pp.245–249. [Online] Available at: http://dx.doi.org/10.1080/1097198X.2015.1108093 [Accessed June 13, 2016].

Ktoridou, D., Eteokleous, N. & Zahariadou, A., 2012. Exploring parents’ and children’s awareness on internet threats in relation to internet safety. *Campus-Wide Information Systems*, Vol. 29(3), pp.133–143. [Online] Available at: www.emeraldinsight.com/doi/abs/10.1108/10650741211243157 [Accessed December 28, 2015].

Kubacki, K., Rundle-Thiele, S., Lahtinen, V. & Parkinson, J., 2015. A systematic review assessing the extent of social marketing principle use in interventions targeting children (2000-2014). *Young Consumers*, Vol. 16(2), pp.141–158. [Online] Available at: http://0-search.ebscohost.com.library.ucc.ie/login.aspx?direct=true&db=psyh&AN=2015-26008-002&site=ehost-live\nk.kubacki@griffith.edu.au [Accessed December 28, 2015].

Kumar, R., 2011. *Research Methodology. A step-by-step guide for beginner.* Third., [Online] Available at: http://books.google.com/books?hl=en&lr=&id=8c6gkbKi-F4C&oi=fnd&pg=PR7&dq=Research+Methodology:+Methods+and+Techniques&ots=iGnHoSUbpN&sig=MCLUW6fq3hl5GDq0RanXjegF9Gg [Accessed June 28, 2015].

Kumari, A., 2014. Evaluating social media as a new tool of journalism education. *South Asia Journal of Multidisciplinary Studies.*, Vol. 1(1), pp.1–10. [Online] Available at: http://gjms.co.in/index.php/SAJMS/article/view/679 [Accessed November 29, 2015].

Kuss, D.J., 2013. Internet gaming addiction: current perspectives. *Psychology Research and Behavior Management*, Vol. 6, pp.125–137. [Online] Available at: https://www.researchgate.net/publication/258768087_Internet_gaming_addiction_Current_perspectives [Accessed June 28, 2016].

Labuschagne, W.A., Burke, I., Veerasamy, N. & Eloff, M.M., 2011. Design of cyber security awareness game utilizing a social media framework. In *2011 Information Security for South Africa*. Ieee, pp. 1–9. [Online] Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6027538 [Accessed June 16, 2014].

Labuschagne, W.A., Eloff, M.M., Veerasamy, N., Leenen, L. & Mujinga, M., 2011. Design of a cyber security awareness campaign for Internet café users in rural areas. In *Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW).* pp. 42–58. [Online] Available at: http://www.academia.edu/29290401/Design_of_a_Cyber_Security_Awareness_Campaign_for_Internet_Café_Users_in_Rural_Areas [Accessed June 16, 2014].

Laczniak, G.R. & Murphy, P.E., 2012. Stakeholder theory and marketing: moving from a firm-centric to a societal perspective. *Journal of Public Policy & Marketing*, Vol.

31(2), pp.1–9. [Online] Available at: http://connection.ebscohost.com/c/articles/83183554/stakeholder-theory-marketing-moving-from-firm-centric-societal-perspective [Accessed June 2, 2015].

Laidre, M.E., Lamb, A., Shultz, S. & Olsen, M., 2013. Making sense of information in noisy networks: human communication, gossip, and distortion. *Journal of Theoretical Biology*, Vol. 317(January), pp.152–160. [Online] Available at: www.sciencedirect.com/science/article/pii/S0022519312004870 [Accessed November 29, 2015].

Lamb, C., Hair, J., McDaniel, C., Boshoff, N., Terblanche, Elliott, R. & Klopper, H., 2015. *Marketing.*, Southern Africa: Oxford University Press.

Laroche, M., Habibi, M.R. & Richard, M., 2013. To be or not to be in social media: how brand loyalty is affected by social media ? *International Journal of Information Management*, Vol. 33(1), pp.76–82. [Online] Available at: http://dx.doi.org/10.1016/j.ijinfomgt.2012.07.003 [Accessed February 11, 2014].

Larson, S., 2015. The cyber security fair: an effective method for training users to improve their cyber security behaviors? *Information Security Education Journal.*, Vol. 2(1), pp.11–19. [Online] Available at: www.dline.info/isej/fulltext/v2n1/2.pdf [Accessed May 20, 2016].

Lavigne, V. & Gouin, D., 2014. Visual analytics for cyber security and intelligence. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, Vol. 11(2), pp.175–199. [Online] Available at: http://dms.sagepub.com/cgi/doi/10.1177/1548512912464532 [Accessed June 13, 2016].

Lebek, B., Uffen, J., Neumann, M., Hohler, B. & H. Breitner, M., 2014. Information security awareness and behavior: a theory-based literature review. *Management Research Review*, Vol. 37(12), pp.1049–1092. [Online] Available at: http://www.emeraldinsight.com/doi/abs/10.1108/MRR-04-2013-0085 [Accessed June 2, 2016].

Lefebvre, R.C., 2013. An integrative model for social marketing. *Journal of Social Marketing*, Vol. 1(1), pp.54–72. [Online] Available at: http://dx.doi.org/10.1108/20426761111104437 [Accessed May 20, 2016].

Leonard, C., 2014. RSG not just for old tannies. *The Media*. [Online] Available at: http://themediaonline.co.za/2014/07/rsg-not-just-for-old-tannies/ [Accessed September 19, 2016].

Lesame, Z. & Seti, V., 2014. Technology access centres and community development: the case of the Eastern Cape province in South Africa. *Mediterranean Journal of Social Sciences*, Vol. 5(10), pp.303–317. [Online] Available at: http://www.mcser.org/journal/index.php/mjss/article/view/2893 [Accessed August 21, 2016].

Leung, L. & Lee, P.S.N., 2012. The influences of information literacy, internet addiction and parenting styles on internet risks. *New Media & Society*, Vol. 14(1), pp.117–136. [Online] Available at: nms.sagepub.com/content/14/1/117.full.pdf [Accessed June 28, 2016].

Levine, E.L., 2013. A study of parental understanding of an intervention in cyberbullying among children in fourth through eighth grade. , pp.1–224. [Online] Available at: https://dspace.iup.edu/handle/2069/1989?show=full [Accessed June 19, 2016].

Lewis, C., 2013. Universal access and service interventions in South Africa: best practice, poor impact. *The African Journal of Information and Communication. Leadership in the electronic age: a broad inter-disciplinary practice.*, (13), pp.95–107. [Online] Available at: http://reference.sabinet.co.za/document/EJC148553 [Accessed July 6, 2016].

Lewis, M.K., 2012. New dogs, old tricks. Why do Ponzi schemes succeed? *Accounting Forum*, Vol. 36(4), pp.294–309. [Online] Available at: http://dx.doi.org/10.1016/j.accfor.2011.11.002 [Accessed September 2, 2016].

Lewis, S., 2015. Qualitative inquiry and research design: choosing among five approaches. *Health Promotion Practice*, Vol. 16(4), pp.473–475. [Online] Available at: hpp.sagepub.com/content/16/4/473.abstract [Accessed September 2, 2016].

Liu, Y.T., Zehtabchi, S. & Liteplo, A.S., 2014. Ultrasound and the six thinking hats. *Academic Emergency Medicine*, Vol. 21(8), pp.920–921. [Online] Available at: www.ncbi.nlm.nih.gov/pubmed/25154709 [Accessed October 16, 2016].

Livingstone, S. & Bulger, M., 2014. A global research agenda for children’s rights in the digital age. *Journal of Children and Media*, Vol. 8(4), pp.317–335. [Online] Available at: http://dx.doi.org/10.1080/17482798.2014.961496 [Accessed June 19, 2016].

Livingstone, S., Davidson, J., Bryce, J., Millwood Hargrave, A. & Grove-Hills, J., 2011. Children’s online activities: risks and safety. *UKCCIS Evidence Group*, pp.1–46. [Online] Available at: www.lse.ac.uk/media@lse/research/EUKidsOnline/...11)/.../UKReport.pdf [Accessed June 26, 2016].

Livingstone, S. & Görzig, A., 2014. When adolescents receive sexual messages on the internet: Explaining experiences of risk and harm. *Computers in Human Behavior*, Vol. 33, pp.8–15. [Online] Available at: http://dx.doi.org/10.1016/j.chb.2013.12.021 [Accessed June 20, 2016].

Lowry, P.B., Wilson, D.W. & Haig, W.L., 2015. A picture is worth a thousand words: source credibility theory applied to logo and website design for heightened credibility and consumer trust. *International Journal of Human-Computer Interaction*, Vol. 30, pp.63–93. [Online] Available at: www.tandfonline.com/doi/pdf/10.1080/10447318.2013.839899 [Accessed July 1, 2016].

Lozano, N., Prades, J. & Montagut, M., 2015. Som la Pera : How to develop a social marketing and public relations campaign to prevent obesity among teenagers in Catalonia. *Catalan Journal of Communication & Cultural Studies.*, Vol. 7(2), pp.251–259. [Online] Available at: doi: 10.1386/cjcs.7.2.251_1 CJCS [Accessed February 16, 2016].

Malterud, K., 2012. Systematic text condensation: a strategy for qualitative analysis. *Scandinavian Journal of Public Health*, Vol. 40(8), pp.795–805. [Online] Available at: http://www.ncbi.nlm.nih.gov/pubmed/23221918 [Accessed August 21, 2016].

Mann, B.J.S. & Ghuman, M.K., 2015. What and how to communicate about a corporate brand with the consumers: an exploratory study. *Journal of Marketing Communications*, (August), pp.1–20. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/13527266.2014.995206 [Accessed May 29, 2016].

Manuputty, A., Noor, S.M. & Sumardi, J., 2013. Cyber security: rule of use Internet safely? *Procedia - Social and Behavioral Sciences*, Vol. 103, pp.255–261. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S1877042813037786 [Accessed May 29, 2016].

Maree, K., 2007. *First steps in research.*, South Africa: Van Schaiks.

Maringe, F., Masinire, a. & Nkambule, T., 2015. Distinctive features of schools in multiple deprived communities in South Africa: Implications for policy and leadership. *Educational Management Administration & Leadership*, Vol. 43(3), pp.363–385. [Online] Available at: http://ema.sagepub.com/cgi/doi/10.1177/1741143215570303.

Mark, L. & Ratliffe, K.T., 2011. Cyber worlds: new playgrounds for bullying. *Computers in the Schools*, Vol. 28(2), pp.92–116. [Online] Available at: www.tandfonline.com/doi/abs/10.1080/07380569.2011.575753 [Accessed June 13, 2016].

Martin, J. & Slane, A., 2015. Child Sexual Abuse Images Online: Confronting the Problem. *Child and Youth Services*, Vol. 36(4), pp.261–266. [Online] Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84949483020&partnerID=40&md5=1f3727d48f848784bcd1f67055162be4.

Martin, N. & Rice, J., 2011. Cybercrime: understanding and addressing the concerns of stakeholders. *Computers and Security*, Vol. 30(8), pp.803–814. [Online] Available at: http://dx.doi.org/10.1016/j.cose.2011.07.003 [Accessed June 20, 2016].

Mashaba, E.K. & Maile, S., 2013. The cost of teacher absenteeism in selected Soshanguve. *International Journal of Arts and Entrepreneurship*, Vol. 1(5), pp.1–25. [Online] Available at: www.ijsse.org/articles/ijsse_v1_i3_171_197.pdf [Accessed August 7, 2016].

Mayasari, I., 2012. The perspectives to understand social marketing as an approach in influencing consumer behavior for good. *Gadjah Mada International Journal of Business*, Vol. 14(2), pp.163–182. [Online] Available at: jurnal.ugm.ac.id/gamaijb/article/view/5442 [Accessed June 2, 2015].

Mazzei, A., 2014. A multidisciplinary approach for a new understanding of corporate communication. *Corporate Communications: An International Journal*, Vol. 19(2), pp.216–230. [Online] Available at: http://www.emeraldinsight.com/10.1108/CCIJ-12-2011-0073 [Accessed June 2, 2015].

McCrohan, K.F., Engel, K. & Harvey, J.W., 2010. Influence of awareness and training on cyber security. *Journal of Internet Commerce*, Vol. 9(1), pp.23–41. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/15332861.2010.487415 [Accessed June 13, 2016].

McGillivray, D., McPherson, G., Jones, J. & McCandlish, A., 2015. Young people, digital media making and critical digital citizenship. *Leisure Studies*, Vol. 4367(November), pp.1–15. [Online] Available at: http://www.tandfonline.com/doi/full/10.1080/02614367.2015.1062041 [Accessed July 1, 2016].

McKay, J., Marshall, P. & Grainger, N., 2014. Rethinking communication in IT project management. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. pp. 4315–4324. [Online] Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6759135&tag=1 [Accessed November 25, 2015].

MediaSmarts, Private pirates. [Online] Available at: http://mediasmarts.ca/game/privacy-pirates-interactive-unit-online-privacy-ages-7-9 [Accessed June 30, 2016].

Menon, S. & Siew, T.G., 2012. Key challenges in tackling economic and cyber crimes: creating a multilateral platform for international co-operation. *Journal of Money Laundering Control*, Vol. 15(3), pp.243–256. [Online] Available at: http://dx.doi.org/10.1108/13685201211238016 [Accessed June 7, 2016].

Mestry, R., 2014. The implications of the National Norms and Standards for School Funding policy on equity in South African public schools. *South African Journal of Education*, Vol. 34(3), pp.1–11. [Online] Available at: http://www.sajournalofeducation.co.za/index.php/saje/article/view/934/444 [Accessed August 20, 2016].

Mestry, R. & Ndhlovu, R., 2014. The implications of the National Norms and Standards for School Funding policy on equity in South African public schools. *South African*

Journal of Education, Vol. 34(3), pp.1–11. [Online] Available at: http://www.sajournalofeducation.co.za/index.php/saje/article/view/934/444.

Miller, B.M., 2010. Community stakeholders and marketplace advocacy: a model of advocacy, agenda building, and industry approval. *Journal of Public Relations Research*, Vol. 22(1), pp.85–112. [Online] Available at: www.tandfonline.com/doi/pdf/10.1080/10627260903170993 [Accessed May 28, 2015].

Mishna, F., Cook, C., Saini, M., Wu, M.-J. & MacFadden, R., 2011. Interventions to prevent and reduce cyber abuse of youth: a systematic review. *Research on Social Work Practice*, Vol. 21(1), pp.5–14. [Online] Available at: http://search.proquest.com.ezproxy.uky.edu/socabs/docview/852138109/13811C03F6B31E815B7/61?accountid=11836\nhttp://apps.webofknowledge.com.ezproxy.uky.edu/full_record.do?product=WOS&search_mode=GeneralSearch&qid=147&SID=3EJKmhDe9L21ffGM28l&page=2&doc=53&c [Accessed February 18, 2016].

Mncube, V. & Madikizela-Madiya, N., 2014. Gangsterism as a cause of violence in South African schools: The case of six provinces. *Journal of Sociology and Social Anthropology*, Vol. 5(1), pp.43–50. [Online] Available at: http://www.krepublishers.com/02-Journals/JSSA/JSSA-05-0-000-14-Web/JSSA-05-1-000-14-Abst-PDF/JSSA-05-1-043-14-025-Mncube-V/JSSA-05-1-043-14-025-Mncube-V-Tt.pdf [Accessed September 14, 2016].

Modisaotsile, B.M., 2012. *The Failing Standard of Basic Education in South Africa*, [Online] Available at: http://www.ai.org.za/wp-content/uploads/downloads/2012/03/No.-72.The-Failing-Standard-of-Basic-Education-in-South-Africa1.pdf [Accessed August 9, 2016].

Mohamad, B., Abu, H., Halim, H., Rageh, A., Bakar, H.A., Halim, H. & Ismail, A.R., 2014. Corporate Communication Management (CCM) and organisational performance: review of the current literature , conceptual model and research propositions. *Procedia - Social and Behavioral Sciences*, Vol. 155(October), pp.115–122. [Online] Available at: http://creativecommons.org/licenses/by-nc-nd/3.0/\nhttp://dx.doi.org/10.1016/j.sbspro.2014.10.266 [Accessed June 9, 2015].

Mohebbi, M., 2014. Investigating the gender-based colour preference in children.

Procedia - Social and Behavioral Sciences, Vol. 112(Iceepsy 2013), pp.827–831. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S1877042814012555 [Accessed May 18, 2016].

Monzani, L., Ripoll, P., Peiró, J.M. & Van Dick, R., 2014. Loafing in the digital age: the role of computer mediated communication in the relation between perceived loafing and group affective outcomes. *Computers in Human Behavior*, Vol. 33, pp.279–285. [Online] Available at: http://dx.doi.org/10.1016/j.chb.2014.01.013 [Accessed June 28, 2016].

Mossberger, K., 2014. Digital citizenship: broadband, mobile use, and activities online. *International Political Science Association Conference, Montreal*, pp.1–30. [Online] Available at: paperroom.ipsa.org/papers/paper_36182.pdf [Accessed July 1, 2016].

Moyo, M., Madzima, K. & Abdullah, H., 2014. Information and Communication Technology integration in classroom teaching: why South African educators lack interest? In *ISTE International Conference on Mathematics, Science and Technology Education.* pp. 378–396. [Online] Available at: https://dspace.nwu.ac.za/bitstream/handle/10394/16116/OA-Ferreira-iste_past-conf-proceedings_2014.pdf?sequence=1&isAllowed=y#page=378 [Accessed July 2, 2016].

Msibi, T., 2012. 'I'm used to it now': experiences of homophobia among queer youth in South African township schools. *Gender and Education*, Vol. 24(5), pp.515–533. [Online] Available at: www.tandfonline.com/doi/full/10.1080/09540253.2011.645021 [Accessed August 7, 2016].

Mthanti, B. & Mncube, V., 2014. The social and economic impact of corporal punishment in South African schools. *Journal of Sociology and Social Anthropology*, Vol. 5(1), pp.71–80. [Online] Available at: www.krepublishers.com/.../JSSA-05-1-071-14-028-Mncube-V-Tt.pdf [Accessed August 21, 2016].

Muda, M., Musa, R. & Putit, L., 2012. Breaking through the Clutter in Media Environment: How Do Celebrities Help? *Procedia - Social and Behavioral*

Sciences, Vol. 42, pp.374–382. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S187704281201083X [Accessed May 21, 2016].

Mukeredzi, T.G. & Mandrona, A.R., 2013. The journey to becoming professionals: Student teachers' experiences of teaching practice in a rural South African context. *International Journal of Educational Research*, Vol. 62, pp.141–151. [Online] Available at: http://dx.doi.org/10.1016/j.ijer.2013.07.010 [Accessed August 19, 2016].

Mulhern, F., 2009. Integrated marketing communications: from media channels to digital connectivity. *Journal of Marketing Communications*, Vol. 15(2–3), pp.85–101. [Online] Available at: www.tandfonline.com/doi/abs/10.1080/13527260902757506 [Accessed June 29, 2015].

Myers, C., Haworth, N. & Hayton, J., 2016. *Helmshore primary policy on child protection.*, UK: Helmshore Primary School. [Online] Available at: http://www.helmshoreprimaryschool.co.uk/wp-content/uploads/2016/01/Child-Protection-Policy-2015-16.pdf [Accessed June 20, 2016].

Nansen, B., Chakraborty, K., Gibbs, L., MacDougall, C. & Vetere, F., 2012. Children and digital wellbeing in Australia: Online regulation, conduct and competence. *Journal of Children and Media*, Vol. 6(2), pp.237–254. [Online] Available at: www.tandfonline.com/doi/abs/10.1080/17482798.2011.619548 [Accessed June 26, 2016].

Naplavova, M., Ludik, T., Hruza, P. & Bozek, F., 2014. General awareness of teenagers in Information Security. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, Vol. 8(11), pp.3415–3418. [Online] Available at: waset.org/publications/.../general-awareness-of-teenagers-in-information-security [Accessed June 26, 2016].

Nathanail, E. & Adamos, G., 2013. Road safety communication campaigns: research designs and behavioral modeling. *Transportation Research Part F: Traffic Psychology and Behaviour*, Vol. 18, pp.107–122. [Online] Available at: http://dx.doi.org/10.1016/j.trf.2012.12.003 [Accessed June 3, 2016].

Nevondwe, L. & Odeku, K.O., 2014. Protecting children from exposure to pornography in South Africa. *Bangladesh e-Journal of Sociology*, Vol. 11(2), pp.132–142. [Online] Available at: www.bangladeshsociology.org/10.11-5.pdf [Accessed June 28, 2016].

NMMU, 2016. NMMU Identity. *NMMU Website*. [Online] Available at: www.nmmu.ac.za/about-nmmu/management/our-identity [Accessed September 10, 2016].

O'Connor, Z., 2015. Colour, contrast and Gestalt theories of perception: The impact in contemporary visual communications design. *Color Research and Application*, Vol. 40(1), pp.85–92. [Online] Available at: onlinelibrary.wiley.com/doi/10.1002/col.21858/abstract [Accessed June 25, 2016].

O'Reilly, M., 2015. *I have a right to privacy. Parental monitoring of adolescents use of social network sites.* [Online] Available at: esource.dbs.ie/handle/10788/2496 [Accessed June 28, 2016].

Ohler, J., 2011. Digital citizenship means character education for the digital age. *Kappa Delta Pi Record*, Vol. 47(Fall), pp.25–27. [Online] Available at: www.tandfonline.com/doi/pdf/10.1080/00228958.2011.10516720 [Accessed July 1, 2016].

Olohunfunmi, I.A. & Fajri, A., 2014. Cyber exploration and hang-out as determinants for adolescents' parental disobedience. *Asian Journal of Social Sciences & Humanities.*, Vol. 3 (4)(November), pp.49–56. [Online] Available at: www.ajssh.leena-luna.co.jp/AJSSHPDFs/Vol.3(4)/AJSSH2014(3.4-06).pdf [Accessed June 29, 2016].

Omar, S.Z., Daud, A., Hassan, M.S., Bolong, J. & Teimmouri, M., 2014. Children Internet usage: opportunities for self development. In *International Conference on Communication and Media 2014 (i-COME'14)*. pp. 75–80. [Online] Available at: www.sciencedirect.com/science/article/pii/S1877042814057255 [Accessed June 7, 2016].

Onwuegbuzie, A.J., Leech, N.L. & Collins, K.M.T., 2012. Qualitative analysis techniques for the review of the literature. *The Qualitative Report*, Vol. 17(56), pp.1–28. [Online] Available at: http://nsuworks.nova.edu/tqr/vol17/iss28/2/ [Accessed August 19, 2015].

Owens, E.W., Behun, R.J., Manning, J.C. & Reid, R.C., 2012. The impact of Internet pornography on adolescents: a review of the research. *Sexual Addiction & Compulsivity*, Vol. 19(1–2), pp.99–122. [Online] Available at: psych.utoronto.ca/users/tafarodi/psy427/articles/Owens et al. (2012).pdf [Accessed June 28, 2016].

Oyedemi, T., 2015. Internet access as citizen's right? Citizenship in the digital age. *Citizenship Studies*, Vol. 19(3/4), pp.450–464. [Online] Available at: 10.1080/13621025.2014.970441\nhttp://0-search.ebscohost.com.mercury.concordia.ca/login.aspx?direct=true&db=a9h&AN=108929702&site=ehost-live&scope=site [Accessed July 1, 2016].

Özgür, H., 2016. The relationship between Internet parenting styles and Internet usage of children and adolescents. *Computers in Human Behavior*, Vol. 60, pp.411–424.

Page, B. & Sharp, A., 2012. The contribution of marketing to school-based program evaluation. *Journal of Social Marketing*, Vol. 2(3), pp.176–186. [Online] Available at: http://www.emeraldinsight.com/10.1108/20426761211265177 [Accessed December 28, 2015].

Pairoa, I. & Arunrangsiwed, P., 2016. The effect of brand mascots on consumers' purchasing behaviors. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, Vol. 10(5), pp.1620–1623. [Online] Available at: waset.org/.../the-effect-of-brand-mascots-on-consumers-purchasing-behaviors [Accessed July 3, 2016].

Palmieri, J., 2016. Cyber five internet safety. [Online] Available at: http://www.abcya.com/cyber_five_internet_safety.htm [Accessed July 3, 2016].

Patterson, A., Khogeer, Y. & Hodgson, J., 2013. How to create an influential anthropomorphic mascot: Literary musings on marketing, make-believe, and meerkats. *Journal of Marketing Management*, Vol. 29(1–2), pp.69–85. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/0267257X.2012.759992 [Accessed July 3, 2015].

Perloff, R.M., 2014. *The Dynamics of Persuasion. Communication and attitudes in the 21st century.* Fifth., Routledge.

Pfleeger, S.L. & Caputo, D.D., 2012. Leveraging behavioral science to mitigate cyber security risk. *Computers and Security*, Vol. 31(4), pp.597–611. [Online] Available at: http://dx.doi.org/10.1016/j.cose.2011.12.010.

Pinar, M., Trapp, P., Girard, T. & Boyt, T.E., 2011. Utilizing the brand ecosystem framework in designing branding strategies for higher education. *International Journal of Educational Management*, Vol. 25, pp.724–739.

Pinto, T., Barreto, J., Praça, I., Sousa, T.M., Vale, Z. & Solteiro Pires, E.J., 2015. Six thinking hats: A novel metalearner for intelligent decision support in electricity markets. *Decision Support Systems*, Vol. 79, pp.1–11. [Online] Available at: http://dx.doi.org/10.1016/j.dss.2015.07.011 [Accessed October 5, 2016].

Platz, M., Krieger, M., Niehaus, E. & Winter, K., 2016. Electronic proofs and electronic assessments in an educational context transferred to South African conditions. In *IST-Africa 2016 Conference Proceedings*. pp. 1–10. [Online] Available at: http://www.ist-africa.org/Conference2016 Page [Accessed August 27, 2016].

Ponelis, S.R. & Holmner, M., 2015. Information Technology for development ICT in Africa: enabling a better life for all. *Information Technology for Development*, Vol. 21(1), pp.1–11. [Online] Available at: http://dx.doi.org/10.1080/02681102.2014.985521 [Accessed June 23, 2016].

Pooley, J.D., 2016. Communication Theory and the Disciplines. *The International Encyclopedia of Communication Theory and Philosophy.*, pp.1–16. [Online] Available at: http://dx.doi.org/10.1002/9781118766804.wbiect261.

Popescu, D.M., Pârgaru, I., Popescu, C. & Mihai, D., 2015. A multidisciplinary approach of communication. *Theoretical and Applied Economics*, Vol. 22(2), pp.65–76. [Online] Available at: http://www.ectap.ro/a-multidisciplinary-approach-of-communication-delia-mioara-popescu_ion-pargaru_constanta-popescu_daniel-mihai/a1083/ [Accessed July 23, 2016].

Popovac, M. & Leoschut, L., 2012. *Cyber bullying in South Africa: impact and responses*, [Online] Available at: http://cjcp.skinthecat.co.za/articlesPDF/63/IssuePaper13-Cyberbullying-SA-Impact_Responses.pdf [Accessed June 29, 2016].

Prakken, H. & Sartor, G., 2015. Law and logic : A review from an argumentation perspective. *Artificial Intelligence*, Vol. 227, pp.214–245. [Online] Available at: http://dx.doi.org/10.1016/j.artint.2015.06.005 [Accessed September 2, 2016].

Pravossoudovitch, K., Cury, F., Young, S.G. & Elliot, A.J., 2014. Is red the colour of danger? Testing an implicit red-danger association. *Ergonomics*, Vol. 57(4), pp.503–10. [Online] Available at: http://www.ncbi.nlm.nih.gov/pubmed/24588355 [Accessed July 2, 2016].

Pruitt-Mentle, D., 2008. *National cyberethics, Ccbersafety, cybersecurity baseline study*,

Pusey, P. & Sadera, W.A., 2011. Cyberethics, cybersafety, and cybersecurity. *Journal of Digital Learning in Teacher Education*, Vol. 28(2), pp.82–85. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/21532974.2011.10784684 [Accessed June 13, 2015].

Qian, Y., Fang, Y. & Gonzalez, J.J., 2012. Managing information security risks during new technology adoption. *Computers & Security*, Vol. 31(8), pp.859–869. [Online] Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404812001368 [Accessed May 25, 2014].

Quigley, K., Burns, C. & Stallard, K., 2013. *Communicating Effectively about Cyber-security Risks: Probabilities, Peer Networks and a Longer Term Education Program.*, [Online] Available at: http://cip.management.dal.ca/wp-content/uploads/2013/04/Quigley-Burns-Stallard-Cyber-Security-Paper-Final-1.pdf.

Quigley, K., Burns, C. & Stallard, K., 2015. ‘Cyber Gurus’: A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, Vol. 32(2), pp.108–117. [Online] Available at: http://dx.doi.org/10.1016/j.giq.2015.02.001 [Accessed June 6, 2016].

Qureshi, S., 2012. As the global digital divide narrows, who is being left behind? *Information Technology for Development*, Vol. 18(4), pp.277–280. [Online] Available at: www.tandfonline.com/doi/pdf/10.1080/02681102.2012.730656 [Accessed June 26, 2016].

Ramnarain, U.D., 2014. Teachers’ perceptions of inquiry-based learning in urban, suburban, township and rural high schools: The context-specificity of science curriculum implementation in South Africa. *Teaching and Teacher Education*, Vol. 38, pp.65–75. [Online] Available at: http://dx.doi.org/10.1016/j.tate.2013.11.003 [Accessed August 9, 2016].

Rantos, K., Fysarakis, K. & Manifavas, C., 2012. How effective is your security awareness program? An evaluation methodology. *Information Security Journal: A Global Perspective*, Vol. 21(6), pp.328–345. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/19393555.2012.747234 [Accessed June 13, 2016].

Raval, Z., Tanna, D. & Raval, D., 2014. Internet marketing over traditional marketing. *International Journal of Software and Hardware Research in Engineering.*, Vol. 2(8), pp.68–73. [Online] Available at: www.academia.edu/17275287/Internet_Marketing_Over_Traditional_Marketing [Accessed June 8, 2016].

Rawal, P., 2013. AIDA Marketing Communication Model: Stimulating a purchase decision in the minds of the consumers through a linear progression of steps. *International Journal of Multidisciplinary Research in Social & Management Sciences*, (1), pp.37–44. [Online] Available at: www.ircjournals.org/vol1/37-44.pdf [Accessed July 1, 2016].

Reid, R. & Van Niekerk, J., 2014a. Snakes and ladders for digital natives: information security education for the youth. *Information Management & Computer Security*, Vol. 22(2), p.179. [Online] Available at: http://search.proquest.com/docview/1660152864?accountid=10610\nhttp://sfxhosted.exlibrisgroup.com/duquesne?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&sid=ProQ:ProQ:abiglobal&atitle=Snakes+and+ladders+for+digital+natives: [Accessed June 2, 2016].

Reid, R. & Van Niekerk, J., 2014b. Towards an education campaign for fostering a societal, cyber security culture. In *8th International Symposium on Human Aspects of Information Security & Assurance*. pp. 174–184. [Online] Available at: https://www.cscan.org/default.asp?page=openaccess&eid=15&id=249 [Accessed June 2, 2016].

Reinold, T. & Tropp, J., 2012. Integrated marketing communications: How can we measure its effectiveness? *Journal of Marketing Communications*, Vol. 18(2), pp.113–132.

Ribble, M. & Miller, T.N., 2013. Educational leadership in an online world: connecting students to technology responsibly, safely, and ethically. *Journal of Asynchronous Learning Network*, Vol. 17(1), pp.137–145. [Online] Available at: eric.ed.gov/?id=EJ1011379 [Accessed July 1, 2016].

Rice, R.E. & Atkin, C.K. eds., 2013. *Public Communication Campaigns*, USA:SAGE.

Ridley, G., 2015. National security as a Corporate Social Responsibility: critical infrastructure resilience. *Jounal of Business Ethics*, Vol. 104(3), pp.361–370. [Online] Available at: link.springer.com/article/10.1007/s10551-011-0845-6 [Accessed June 2, 2016].

Riege, A.M., 2003. Validity and reliability tests in case study research: a literature review with ‘hands-on’ applications for each research phase. *Qualitative Market Research: An International Journal*, Vol. 6(2), pp.75–86. [Online] Available at: www.emeraldinsight.com/doi/pdf/10.1108/13522750310470055 [Accessed June 2, 2015].

Rikkers, W., Lawrence, D., Hafekost, J. & Zubrick, S.R., 2016. Internet use and electronic gaming by children and adolescents with emotional and behavioural problems in Australia – results from the second child and adolescent survey of mental health and wellbeing. *BMC Public Health*, Vol. 16(1), pp.2–16. [Online] Available at: http://bmcpublichealth.biomedcentral.com/articles/10.1186/s12889-016-3058-1 [Accessed June 28, 2016].

Rowley, J., 2002. Using Case Studies in Research. *Management Research News*, Vol. 25(1), pp.16–27. [Online] Available at: http://www.emeraldinsight.com/doi/abs/10.1108/01409170210782990 [Accessed June 2, 2015].

Rudi, J., Dworkin, J., Walker, S. & Doty, J., 2014. Parents’ use of information and communications technologies for family communication: differences by age of children. *Information, Communication & Society*, Vol. 4462(August 2014), pp.1–16. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/1369118X.2014.934390 [Accessed June 2, 2016].

Rule, P. & John, V.M., 2015. A necessary dialogue: theory in case study research. *International Journal of Qualitative Methods*, Vol. 14(4), pp.1–11. [Online] Available at: ijq.sagepub.com/content/14/4/1609406915611575.abstract [Accessed June 2, 2015].

Rule, P. & John, V.M., 2011. *Your guide to case study research.*, Pretoria: Van Schaik.

Saeed, R., Naeem, B., Bilal, M. & Naz, U., 2013. Integrated marketing communication : a review paper. *Interdisciplinary Journal of Contemporary Research in Business*, Vol. 5(5), pp.124–133. [Online] Available at: journal-archieves35.webs.com/124-133.pdf [Accessed June 26, 2016].

Saladin-Subero, R. & Hawkins, K., 2011. Stop bullying now! Campaign pilot evaluation: A qualitative assessment of its usefulness and cultural appropriateness for Hispanic populations. *Social Marketing Quarterly*, Vol. 17(2), pp.2–18. [Online] Available at: http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=psyh&AN=2011-11528-001&site=ehost-live&custid=s4121186 [Accessed June 9, 2015].

Salamzada, K., Shukur, Z. & Bakar, M.A.B.U., 2015. A framework for cybersecurity strategy for developing countries: case study of Afghanistan. *Asia-Pacific Journal of Information Technology and Multimedia*, Vol. 4(1), pp.1–10. [Online] Available at: http://ejournals.ukm.my/apjitm/article/view/6503/3189 [Accessed June 29, 2016].

Saridakis, G., Benson, V., Ezingeard, J.N. & Tennakoon, H., 2016. Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, Vol. 102, pp.320–330. [Online] Available at: http://dx.doi.org/10.1016/j.techfore.2015.08.012 [Accessed June 7, 2016].

Sasson, H. & Mesch, G., 2014. Parental mediation, peer norms and risky online behavior among adolescents. *Computers in Human Behavior*, Vol. 33, pp.32–38. [Online] Available at: http://dx.doi.org/10.1016/j.chb.2013.12.025 [Accessed June 28, 2015].

Schia, N.N., 2016. *Teach a person how to surf: cyber security as development assistance*, [Online] Available at: https://brage.bibsys.no/xmlui/bitstream/id/.../NUPI_Report_4_16_Nagelhus_Schia

.pdf [Accessed June 29, 2016].

Schreier, M., 2012. *Qualitative Content Analysis in Practice.*, UK: SAGE.

Sezer, B., Yilmaz, R. & Yilmaz, F.G.K., 2015. Cyber bullying and teachers' awareness. *Internet Research*, Vol. 25(4), p.674. [Online] Available at: http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=108405378&site=eds-live [Accessed December 28, 2015].

Shackelford, S.J. & Fort, T.L., 2011. *Sustainable cybersecurity: applying lessons from the green movement to managing cyber attacks.*, [Online] Available at: http://dx.doi.org/10.2139/ssrn.2324620 [Accessed June 28, 2016].

Shava, F.B. & Van Greunen, D., 2013. Factors affecting user experience with security features: A case study of an academic institution in Namibia. In *2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference*. pp. 1–8. [Online] Available at: http://icsa.cs.up.ac.za/issa/2013/Proceedings/Full/69/69_Paper.pdf [Accessed August 21, 2016].

Sheperd, S., 2011. White House conference tackles bullying. [Online] Available at: http://edition.cnn.com/2011/POLITICS/03/10/obama.bullying/ [Accessed October 26, 2016].

Shepherd, D., 2015. Learn to teach, teach to learn: A within-pupil across -subject approach to estimating the impact of teacher subject knowledge on South African grade 6 performance. In Stellenbosch Economic Working Papers. pp. 1–42. [Online] Available at: www.ekon.sun.ac.za/wpapers/2015/wp012015/wp-01-2015.pdf [Accessed August 19, 2016].

Shields, N., Nadasen, K. & Hanneke, C., 2014. Teacher Responses to School Violence in Cape Town, South Africa. *Journal of Applied Social Science*, pp.1–18. [Online] Available at: jax.sagepub.com/content/early/2014/04/20/1936724414528181.refs [Accessed August 9, 2016].

Shifrin, D., Brown, A., Hill, D., Jana, L. & Flinn, S.K., 2015. Growing Up Digital : Media Research Symposium. In *Growing up digital: Media research symposium*. American Academy of Pediatrics, pp. 1–7. [Online] Available at:

https://www.aap.org/en-us/Documents/digital_media_symposium_proceedings.pdf [Accessed July 1, 2016].

Shillair, R., Cotten, S.R., Tsai, H.S., Alhabash, S., LaRose, R. & Rifon, N.J., 2015. Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, Vol. 48, pp.199–207. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S0747563215000606 [Accessed October 18, 2015].

Simons, H., 2015. Interpret in context: Generalizing from the single case in evaluation. *Evaluation*, Vol. 21(2), pp.173–188. [Online] Available at: http://evi.sagepub.com.ez.sun.ac.za/content/21/2/173.short [Accessed February 18, 2016].

Simsek, E. & Simsek, A., 2013. New literacies for digital citizenship. *Contemporary Educational Technology*, Vol. 4(2), pp.126–137. [Online] Available at: http://eric.ed.gov/?id=ED542213 [Accessed July 1, 2016].

Singh, M., 2012. Marketing Mix of 4P ' S for Competitive Advantage. *IOSR Journal of Business and Management (IOSRJBM)*, Vol. 3(6), pp.40–45. [Online] Available at: www.iosrjournals.org [Accessed June 2, 2015].

Singh, N. & Rishi, A., 2015. Pyramid: A Case Study of Cyber Security in India. *South Asian Journal of Business and Management Cases*, Vol. 4(1), pp.135–142. [Online] Available at: bmc.sagepub.com/content/4/1/135.abstract [Accessed February 18, 2016].

Siomos, K., Floros, G., Fisoun, V., Evaggelia, D., Farkonas, N., Sergentani, E., Lamprou, M. & Geroukalis, D., 2012. Evolution of Internet addiction in Greek adolescent students over a two-year period: The impact of parental bonding. *European Child and Adolescent Psychiatry*, Vol. 21(4), pp.211–219. [Online] Available at: https://www.ncbi.nlm.nih.gov/pubmed/22311146 [Accessed December 28, 2015].

Skelton, A., 2014. Leveraging funds for school infrastructure: The South African 'mud schools' case study. *International Journal of Educational Development*, Vol. 39(2014), pp.59–63. [Online] Available at:

http://dx.doi.org/10.1016/j.ijedudev.2014.07.008 [Accessed August 20, 2016].

Skinner, C., Mersham, G. & Benecke, R., 2013. *Handbook of Public Relations.* 10th ed., Southern Africa: Oxford University Press.

Skopik, F., Settanni, G. & Fiedler, R., 2016. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, Vol. 60, pp.154–176. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S0167404816300347 [Accessed June 7, 2016].

Slonje, R., Smith, P.K. & Frisén, A., 2013. Computers in human behavior the nature of cyberbullying , and strategies for prevention. *Computers in Human Behavior*, Vol. 29(1), pp.26–32. [Online] Available at: dl.acm.org/citation.cfm?id=2397390 [Accessed June 2, 2016].

Slusky, L. & Partow-Navid, P., 2012. Students Information Security Practices and Awareness. *Journal of Information Privacy & Security*, Vol. 8(4), pp.3–26. [Online] Available at: http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=85866240&site=ehost-live&scope=site [Accessed June 13, 2016].

Smit, D.M., 2015. Cyberbullying in South African and American schools: A legal comparative study. *South African Journal of Education*, Vol. 35(2), pp.1–11. [Online] Available at: http://www.sajournalofeducation.co.za/index.php/saje/article/view/1076/542 [Accessed August 21, 2016].

Smith, B.G., 2012. Organic integration: the natural process underlying communication integration. *Journal of Communication Management*, Vol. 16(1), pp.4–19. [Online] Available at: http://www.emeraldinsight.com/doi/abs/10.1108/13632541211198012 [Accessed July 3, 2015].

Smith, B.G., 2013. The public relations contribution to IMC: Deriving opportunities from threats and solidifying public relations' future. *Public Relations Review*, Vol. 39(5), pp.507–513. [Online] Available at: http://linkinghub.elsevier.com/retrieve/pii/S0363811113001367 [Accessed

January 27, 2014].

Sommerfeldt, E.J., Kent, M.L. & Taylor, M., 2012. Activist practitioner perspectives of website public relations: Why aren't activist websites fulfilling the dialogic promise? *Public Relations Review*, Vol. 38(2), pp.303–312. [Online] Available at: http://linkinghub.elsevier.com/retrieve/pii/S0363811112000045 [Accessed February 3, 2014].

Sonhera, N., Kritzinger, E. & Loock, M., 2015. Cyber threat incident handling procedure for South African schools. In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA)*. pp. 215–232. [Online] Available at: https://www.cscan.org/openaccess/?id=272 [Accessed June 7, 2016].

South African Cyber Security Academic Alliance, 2016. SACSAA website. [Online] Available at: http://www.cyberaware.org.za/ [Accessed December 28, 2016].

Spaull, N., 2013. Primary school inequality in South Africa. *International Journal of Educational Development*, Vol. 33(5), pp.436–447. [Online] Available at: http://dx.doi.org/10.1016/j.ijedudev.2012.09.009 [Accessed August 7, 2016].

Šramová, B., 2015. Marketing and Media Communications Targeted to Children as Consumers. *Procedia - Social and Behavioral Sciences*, Vol. 191, pp.1522–1527. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S1877042815028281 [Accessed June 7, 2016].

Starcevic, V., 2013. Is Internet addiction a useful concept? *The Australian and New Zealand journal of psychiatry*, Vol. 47(1), pp.16–9. [Online] Available at: http://www.ncbi.nlm.nih.gov/pubmed/23293309 [Accessed June 26, 2016].

Stewart, G. & Lacey, D., 2012. Death by a thousand facts. *Information Management & Computer Security*, Vol. 20(1), pp.29–38. [Online] Available at: http://www.emeraldinsight.com/doi/full/10.1108/09685221211219182 [Accessed June 7, 2016].

Stork, C., Calandro, E. & Gillwald, A., 2013. Internet going mobile: internet access and use in 11 African countries. *Info Journal*, Vol. 15(5), pp.34–51. [Online] Available at: http://www.emeraldinsight.com/10.1108/info-05-2013-0026 [Accessed August

18, 2016].

Strate, L., 1999. The varieties of cyberspace: problems in definition and delimitation. *Western Journal of Communication.*, Vol. 63(3), pp.382–412. [Online] Available at: http://www.ncbi.nlm.nih.gov/pubmed/10912254 [Accessed November 15, 2015].

Strawser, B.J. & Joy, D.J., 2015. Cyber security and user responsibility: surprising normative differences. *Procedia Manufacturing*, Vol. 3, pp.1101–1108. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S2351978915001845 [Accessed June 7, 2016].

Subrahmanyam, K., Reich, S.M., Waechter, N. & Espinoza, G., 2008. Online and offline social networks: Use of social networking sites by emerging adults. *Journal of Applied Developmental Psychology*, Vol. 29(6), pp.420–433. [Online] Available at: http://linkinghub.elsevier.com/retrieve/pii/S0193397308000713 [Accessed February 3, 2014].

Such, J.M., Gouglidis, A., Knowles, W., Misra, G. & Rashid, A., 2016. Information assurance techniques: Perceived cost effectiveness. *Computers and Security*, Vol. 60, pp.117–133. [Online] Available at: http://dx.doi.org/10.1016/j.cose.2016.03.009 [Accessed June 7, 2016].

Sulaiman, A.N.., Moideen, A.I. & Moreira, S.D., 2016. Of Ponzi schemes and investment scams A case study of enforcement actions in Malaysia. *Journal of Financial Crime.*, Vol. 23(1), pp.231–243. [Online] Available at: http://dx.doi.org/10.1108/JFC-05-2014-0021 [Accessed September 2, 2016].

Sullivan, C., 2016. Digital citizenship and the right to digital identity under international law. *Computer Law and Security Review*, Vol. 32(3), pp.474–481. [Online] Available at: http://dx.doi.org/10.1016/j.clsr.2016.02.001 [Accessed July 1, 2016].

Swart, I., Irwin, B. & Grobler, M., 2014. Towards a platform to visualize the state of South Africa ' s information security. In *Information Security for South Africa.* pp. 1–8. [Online] Available at: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6940061 [Accessed June 7, 2016].

Tallapragada, M., Misaras, I.C., Burke, K. & Waters, R.D., 2012. Identifying the best practices of media catching: A national survey of media relations practitioners. *Public Relations Review*, Vol. 38(5), pp.926–931. [Online] Available at: http://linkinghub.elsevier.com/retrieve/pii/S0363811112001488 [Accessed February 3, 2014].

Taylor, C.R., 2013. Editorial: Hot topics in advertising research. *International Journal of Advertising*, Vol. 32(1), pp.6–12. [Online] Available at: www.tandfonline.com/doi/abs/10.2501/IJA-32-1-007-012 [Accessed June 8, 2015].

Teimouri, M., Hassan, M.S., Bolong, J., Daud, A., Yussuf, S. & Adzharuddin, N.A., 2014. What is upsetting our children online? *Procedia - Social and Behavioral Sciences*, Vol. 155, pp.411–416. [Online] Available at: www.sciencedirect.com/science/article/pii/S1877042814057802 [Accessed June 7, 2016].

Thaler, J. & Helmig, B., 2013. Theoretical framework of social marketing effectiveness: drawing the big picture on its functioning. *Journal of Nonprofit & Public Sector Marketing*, Vol. 25(3), pp.211–236. [Online] Available at: http://www.tandfonline.com.acces.bibl.ulaval.ca/doi/abs/10.1080/10495142.2013.819708#.U85rroB5O4k [Accessed July 6, 2016].

Thomas, G., 2011. A Typology for the Case Study in Social Science Following a Review of Definition, Discourse, and Structure. *Qualitative Inquiry*, Vol. 17(6), pp.511–521.

Thomas, J. & Kielman, J., 2009. Challenges for visual analytics. *Information Visualization*, Vol. 8(4), pp.309–314. [Online] Available at: http://ivi.sagepub.com/content/8/4/309 [Accessed June 13, 2016].

Tikk, E., 2011. Ten rules for cyber security. *Survival*, Vol. 53(September 2013), pp.119–132. [Online] Available at: citizenlab.org/cybernorms2011/rules.pdf [Accessed June 13, 2016].

Toledano, M., 2010. Professional competition and cooperation in the digital age: A pilot study of New Zealand practitioners. *Public Relations Review*, Vol. 36(3), pp.230–237. [Online] Available at: http://linkinghub.elsevier.com/retrieve/pii/S0363811110000512 [Accessed

February 3, 2014].

Tomczyk, Ł. & Kopecký, K., 2016. Children and youth safety on the Internet: Experiences from Czech Republic and Poland. *Telematics and Informatics*, Vol. 33(3), pp.822–833. [Online] Available at: www.sciencedirect.com/science/article/pii/S0736585315301143 [Accessed June 3, 2016].

Tracy, S.J., 2013. *Qualitative research methods. Collecting evidence, crafting analysis, communicating impact.*, UK: Wiley-Blackwell.

Trudell, B., 2016. Language choice and education quality in Eastern and Southern Africa: a review. *Comparative Education*, Vol. 52(3), pp.281–293. [Online] Available at: http://www.tandfonline.com/doi/full/10.1080/03050068.2016.1185252 [Accessed June 3, 2016].

Tsitsika, A., Janikian, M., Schoenmakers, T.M., Tzavela, E.C., Olafsson, K., Wójcik, S., Macarie, G.F., Tzavara, C. & Richardson, C., 2014. Internet addictive behavior in adolescence: a cross-sectional study in seven European countries. *Cyberpsychology, behavior and social networking*, Vol. 17(8), pp.528–35. [Online] Available at: http://www.ncbi.nlm.nih.gov/pubmed/24853789 [Accessed June 28, 2015].

Tustin, D.H., Zulu, G.N. & Basson, A., 2014. Bullying among secondary school learners in South Africa with specific emphasis on cyber bullying. *Child Abuse Research: A South African Journal*, Vol. 15(2), pp.13–25. [Online] Available at: http://journals.co.za/deliver/fulltext/carsa/15/2/carsa_v15_n2_a2.pdf;jsessionid=oKosf9VeXo2H1Tu3HvYW9EG0.sabinetlive?itemId=/content/carsa/15/2/EJC161329mimeType=application/pdf [Accessed June 28, 2016].

Tuukkanen, T. & Wilska, T.-A., 2015. Online environments in children’s everyday lives: children’s, parents’ and teachers’ points of view. *Young Consumers*, Vol. 16(1), pp.3–16. [Online] Available at: http://www.emeraldinsight.com/doi/abs/10.1108/YC-03-2014-00430.

Unicef, 2012. *South African mobile generation Study on South African young people on mobiles*, [Online] Available at: http://www.unicef.org/southafrica/SAF_resources_mobilegeneration.pdf [Accessed August 20, 2016].

University of Johannesburg, 2016. Centre for Cyber Security. *Von Solms, B.* [Online] Available at: http://adam.uj.ac.za/csi/ [Accessed August 21, 2016].

Urwin, B. & Venter, M., 2014. Shock advertising: Not so shocking anymore. An investigation among Generation Y. *Mediterranean Journal of Social Sciences*, Vol. 5(21), pp.203–214. [Online] Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84908391303&partnerID=40&md5=83925df017517393e5bf474ad0149b36 [Accessed June 8, 2016].

Vaala, S.E. & Bleakley, A., 2015. Monitoring, Mediating, and Modeling: Parental Influence on Adolescent Computer and Internet Use in the United States. *Journal of Children and Media*, Vol. 9(March), pp.40–57. [Online] Available at: http://dx.doi.org/10.1080/17482798.2015.997103 [Accessed June 28, 2016].

Vanderhoven, E., Schellens, T. & Valcke, M., 2014. Developing educational materials about the risks on social network sites: a design-based research approach. *You are not alone, Abstracts*, Vol. 64(3), pp.459–480. [Online] Available at: http://www.spion.me/finalWorkshop/ [Accessed June 28, 2016].

Van Niekerk, J., Thomson, K.L. & Reid, R., 2013. Cyber safety for school children: A case study in the Nelson Mandela Metropolis. *IFIP Advances in Information and Communication Technology*, Vol. 406, pp.103–112. [Online] Available at: http://link.springer.com/chapter/10.1007/978-3-642-39377-8_11 [Accessed June 2, 2016].

Van Niekerk, M. & Blignaut, S., 2014. A framework for Information and Communication Technology integration in schools through teacher professional development. *Africa Education Review*, Vol. 11(2), pp.236–253. [Online] Available at: http://dx.doi.org/10.1080/18146627.2014.927159 [Accessed June 5, 2015].

Verbeke, A. & Tung, V., 2013. The future of stakeholder management theory: A temporal perspective. *Journal of Business Ethics*, Vol. 112(3), pp.529–543. [Online] Available at: link.springer.com/article/10.1007/s10551-012-1276-8 [Accessed July 3, 2015].

Vernuccio, M., 2014. Communicating corporate brands through social media: an exploratory study. *International Journal of business communication*, Vol. 51, pp.211–233. [Online] Available at:

http://job.sagepub.com/content/51/3/211.abstract [Accessed June 2, 2015].

Vivolo-Kantor, A.M., Martell, B.N., Holland, K.M. & Westby, R., 2014. A systematic review and content analysis of bullying and cyber-bullying measurement strategies. *Aggression and Violent Behavior*, Vol. 19(4), pp.423–434. [Online] Available at: http://www.sciencedirect.com/science/article/pii/S1359178914000615 [Accessed June 7, 2016].

Vlăduțescu, Ștefan, 2013. Message as fundamental discursive commitment of communication. *Journal of Studies in Social Sciences.*, Vol. 5(2), pp.276–287. [Online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732062 [Accessed July 1, 2016].

Vlok, P., 2014. Be cyber smart. *You Magazine*, (3 November). [Online] Available at: http://www.you.co.za/mobile/hey-you/be-cyber-smart/ The [Accessed September 16, 2016].

Von Solms, R. & Van Niekerk, J., 2013. From information security to cyber security. *Computers & Security*, Vol. 38, pp.97–102. [Online] Available at: http://dx.doi.org/10.1016/j.cose.2013.04.004 [Accessed June 7, 2016].

Von Solms, S. & Von Solms, R., 2014. Towards cyber safety education in primary schools in Africa. In *Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance.* pp. 185–197. [Online] Available at: http://books.google.com/books?hl=en&lr=&id=EF_pBgAAQBAJ&oi=fnd&pg=PA185&dq=Towards+Cyber+Safety+Education+in+Primary+Schools+in+Africa&ots=ZnxVnVdtoI&sig=mtumkTGRH0gpaKB_akcD2P95sMU [Accessed June 7, 2016].

Walaza, M., Loock, M. & Kritzinger, E., 2014. A Framework to Integrate ICT Security Awareness into the South African Schooling System. In *Southern African Institute for Computer Scientist and Information Technologists Annual Conference, SAICSIT 2014*. pp. 11–18. [Online] Available at: https://unisa.pure.elsevier.com/en/publications/a-framework-to-integrate-ict-security-awareness-into-the-south-af [Accessed June 7, 2016].

Waller, R., Gardner, F. & Cluver, L., 2014. Shared and unique predictors of antisocial and substance use behavior among a nationally representative sample of South African youth. *Aggression and Violent Behavior*, Vol. 19(6), pp.629–636. [Online] Available at: http://dx.doi.org/10.1016/j.avb.2014.09.002 [Accessed December 28, 2015].

Walter, B.L., 2014. Corporate social responsibility communication: Towards a phase model of strategic planning. *Critical Studies on Corporate Responsibility, Governance and Sustainability*, Vol. 6, pp.59–79. [Online] Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84896501223&partnerID=40&md5=7178810850a64f335e4a1401226cffcc [Accessed August 21, 2015].

Watkins, D.C., 2012. Qualitative Research: The Importance of Conducting Research That Doesn't 'Count'. *Health Promotion Practice*, Vol. 13(2), pp.153–158. [Online] Available at: http://www.academia.edu/4212311/Qualitative_Research_The_Importance_of_Conducting_Research_That_Doesn_t_Count [Accessed August 21, 2015].

Watson, T., 2012. The evolution of public relations measurement and evaluation. *Public Relations Review*, Vol. 38(3), pp.390–398. [Online] Available at: http://linkinghub.elsevier.com/retrieve/pii/S036381111100213X [Accessed January 27, 2014].

Werder, K.P., 2015. The Integration of Domains: Multidisciplinary Approaches to Strategic Communication Campaigns. *International Journal of Strategic Communication*, Vol. 9(2), pp.79–86. [Online] Available at: http://www.tandfonline.com/doi/full/10.1080/1553118X.2015.1010829 [Accessed June 8, 2015].

Whittle, H., Hamilton-Giachritsis, C., Beech, A. & Collings, G., 2013. A review of young people's vulnerabilities to online grooming. *Aggression and Violent Behavior*, Vol. 18(1), pp.135–146. [Online] Available at: http://dx.doi.org/10.1016/j.avb.2012.11.008 [Accessed June 28, 2016].

Wilcox, D.. & Cameron, G.T., 2014. *Public Relations Strategies and Tactics.* Eleventh., USA: Pearson Education Limited.

Williams, A., 2014. Cyber safety awareness on the rise. *The Eastern Cape Herald.* [Online] Available at: http://www.heraldlive.co.za/news/2014/10/16/cyber-safety-awareness-rise/ [Accessed October 16, 2016].

Willis, N. et al., 2013. ‘Communicate to vaccinate’: the development of a taxonomy of communication interventions to improve routine childhood vaccination. *BMC international health and human rights*, Vol. 13, p.23. [Online] Available at: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3655915&tool=pmcentrez&rendertype=abstract [Accessed June 28, 2015].

Winn, M.R., 2012. Promote digital citizenship through school-based social networking. *Learning & Leading with Technology*, Vol. 39(4), pp.10–13. [Online] Available at: http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ954323&lang=it&site=ehost-live&scope=site [Accessed July 1, 2016].

Wong, Y.C., 2010. Cyber-parenting: Internet benefits, risks and parenting issues. *Journal of Technology in Human Services*, Vol. 28(4), pp.252–273. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/15228835.2011.562629 [Accessed June 28, 2016].

Woodside, A.G., 2010. *Case Study Research: Theory, Methods, Practice.*, Emerald Group Publishing Limited.

Xu, Z. & Zhang, W., 2012. Victimized by phishing: A heuristic-systematic perspective. *Journal of Internet Banking and Commerce*, Vol. 17(3), pp.1–16. [Online] Available at: http://www.icommercecentral.com/open-access/victimized-by-phishing-a-heuristicsystematic-perspective.php?aid=38108 [Accessed June 2, 2016].

Yamamoto, J. & Ananou, S., 2015. Humanity in the digital age: cognitive, social, emotional, and ethical implications. *Contemporary Educational Technology*, Vol. 6(1), pp.1–18. [Online] Available at: www.cedtech.net/articles/61/611.pdf [Accessed July 1, 2016].

Yan, C., Dillard, J.P. & Shen, F., 2012. Emotion, motivation, and the persuasive effects of message framing. *Journal of Communication*, Vol. 62(4), pp.682–700. [Online] Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1460-2466.2012.01655.x/abstract [Accessed June 2, 2016].

Yin, R.K., 2013. Validity and generalization in future case study evaluations. *Journal of Evaluation.*, Vol. 19(3), pp.321–332. [Online] Available at:

http://evi.sagepub.com/cgi/doi/10.1177/1356389013497081 [Accessed June 15, 2016].

Yoon, H.J. & Tinkham, S.F., 2013. Humorous Threat Persuasion in Advertising: The Effects of Humor, Threat Intensity, and Issue Involvement. *Journal of Advertising*, Vol. 42(1), pp.30–41. [Online] Available at: http://www.tandfonline.com/doi/abs/10.1080/00913367.2012.749082 [Accessed June 2, 2015].

York, L., 2014. Future focussed teacher education. *Proceedings of the SITE International Symposium*, (April), pp.71–79. [Online] Available at: http://apo.org.au/files/Resource/ebook_149921-1_albion.pdf [Accessed June 28, 2016].

Yusuf, S., Osman, M.N., Hassan, M.S.H. & Teimoury, M., 2014. Parents' Influence on Children's Online Usage. *Procedia - Social and Behavioral Sciences*, Vol. 155, pp.81–86.

Zhu, J., Zhang, W., Yu, C. & Bao, Z., 2015. Early adolescent Internet game addiction in context: How parents, school, and peers impact youth. *Computers in Human Behavior*, Vol. 50, pp.159–168. [Online] Available at: http://dx.doi.org/10.1016/j.chb.2015.03.079 [Accessed February 24, 2016].

Zimmerman, L., 2014. Lessons learnt: Observation of Grade 4 reading comprehension teaching in South African schools across the Progress in International Reading Literacy Study (PIRLS) 2006 achievement spectrum. *Reading & Writing*, Vol. 5(1), pp.4–9. [Online] Available at: http://www.rw.org.za/index.php/rw/article/view/48/109 [Accessed May 20, 2016].

APPENDIX A: PERMISSION FROM SACSAA TO CONDUCT STUDY

SACSAA
South African Cyber Security
Academic Alliance

Prof R von Solms
Director
South African Cyber-security Academic Alliance
E-mail: Rossouw.VonSolms@nmmu.ac.za
Tel: 041 504 3604

18 April 2016

Dear Ms Leppan

We have received your letter dated 4 April 2016, requesting written consent to use the South African Cyber-security Academic Alliance (SACSAA) cyber-security campaign as a case study for your master's study and to obtain access to any campaign content which is not available on the cyberaware.org.za website.

On behalf of all the directors of SACSAA, I grant you permission to use the SACSAA cyber-security campaign as a case study for your research.

If we can assist in any manner with your research project, please do not hesitate to approach us again.

Yours sincerely,

Prof Rossouw von Solms