University of Fort Hare

Together in Excellence

An Information Security Policy Compliance Reinforcement and Assessment Framework

Tapiwa Gundu

2017

An Information Security Policy Compliance Reinforcement and Assessment Framework

By

Tapiwa Gundu

Thesis

submitted in fulfilment of the requirements for the degree

Doctor of Philosophy

in

Information Systems

in the

Faculty of Management and Commerce

at the

University of Fort Hare

Supervisor: **Prof. S. Flowerday**

May 2017

ABSTRACT

The majority of SMEs have adopted the use of information communication and technology (ICT) services. However, this has exposed their systems to new internal and external security vulnerabilities. These SMEs seem more concerned with external threat related vulnerabilities rather than those from internal threats, although researchers and industry are suggesting a substantial proportion of security incidents to be originating from insiders. Internal threat is often addressed by, firstly, a security policy in order to direct activities and, secondly, organisational information security training and awareness programmes. These two approaches aim to ensure that employees are proficient in their roles and that they know how to carry out their responsibilities securely. There has been a significant amount of research conducted to ensure that information security programmes communicate the information security policy effectively and reinforce sound security practice. However, an assessment of the genuine effectiveness of such programmes is seldom carried out. The purposes of this research study were, firstly, to highlight the flaws in assessing behavioural intentions and equating such behavioural intentions with actual behaviours in information security; secondly, to present an information security policy compliance reinforcement and assessment framework which assists in promoting the conversion of intentions into actual behaviours and in assessing the behavioural change. The approach used was based on the Theory of Planned Behaviour, knowledge, attitude and behaviour theory and Deterrence Theory. Expert review and action research methods were used to validate and refine the framework. The action research was rigorously conducted in four iterations at an SME in South Africa and involved 30 participating employees. The main findings of the study revealed that even though employees may have been well trained and are aware of information security good practice, they may be either unable or unwilling to comply with such practice. The findings of the study also revealed that awareness drives which lead to secure behavioural intents are merely a first step in information security compliance. The study found that not all behavioural intentions converted to actual secure behaviours and only 64% converted. However, deterrence using rewards for good behaviour and punishment for undesirable behaviour was able to increase the conversion by 21%.

DECLARATION

I, Tapiwa Gundu (Student Number 200411454), hereby declare that:

- The work in this thesis is my own work.
- All sources used or referred to have been documented.
- I am fully aware of the University of Fort Hare's policy on plagiarism and I have taken every precaution to comply with the regulations.
- This thesis has not been previously submitted in full or partial requirements for an equivalent or higher qualification.
- I am fully aware of the University of Fort Hare's policy on research ethics and I have taken every precaution to comply with the regulations. In addition, I received approval from Fort Hare's Research Ethics Committee to conduct the study (UREC) – (Ref: FLO051SGUN01)

_____ _____

Signature Date

PUBLICATIONS

Journal

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, *104*(2), 69-79.

Gundu, T., Flowerday, S. V. (2017). Deterrence Theory: Bridging the Gap between Intention to Information Security Compliance. (Under Review)

Gundu, T., Flowerday, S. V., and Renaud, K. (2017). Gauging Information Security Compliance: Acknowledging and Appraising the Fallout between Intention and Practice. (Under Review)

ACKNOWLEDGEMENTS

The journey towards a doctoral degree is not an easy one and requires much hard work and considerable sacrifices. However, I was fortunate that my doctoral journey was not a lonely one. Several special people walked with me throughout the journey. My utmost gratitude and appreciation goes to the following:

- To God my creator for giving me strength courage, protection and wisdom. Without your grace and mercy could not have been done. '*handina raki, asi ndakakomborerwa'*.
- To my supervisor, Prof. Stephen Flowerday. Thank you for being a mentor, teacher and friend. I learnt a lot through this experience. You are an excellent mentor who sees potential in people and helps bring out the best in them.
- To the civil engineering organisation where the empirical work was conducted.
- All the information systems masters, doctoral students and staff for assisting me whenever I needed help.
- To Tim Stones and Alexa Barnby, thank you for assistance with language editing and proofreading.
- Finally, my wife Babalwa, Mum, my brother and sister, thank you for all the love, support and prayers.

TABLE OF CONTENTS

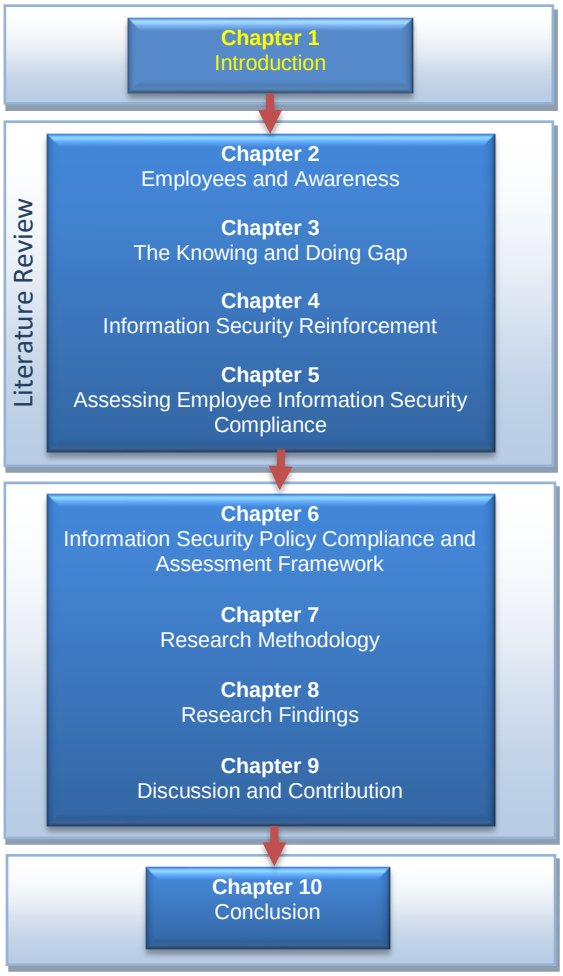
LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ATM	Automated Teller Machine
AR	Action Research
BI	Behavioural Intent
BIS	Business Information Systems
BYOD	Bring Your Own Device
CD-ROM	Compact Disc Read Only Memory
DoS	Denial of Service
DT	Deterrence Theory
DVD	Digital Video Disc
GIS	Geographical Information Systems
ICT	Information and Communication Technology
IS	Information Systems
ISM	Information Security Management
ISP	Information Security Policy
IT	Information Technology
KAB	Knowledge Attitude Behaviour
LA	Level of Awareness
LAN	Local Area Network
PDF	Portable Document Format
PMT	Protection Motivation Theory
SME	Small to Medium Enterprises
SN	Subjective Norm
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
URL	Uniform Resource Locator

CHAPTER 1 - INTRODUCTION



Chapter 1:

This is an introductory chapter and provides an overview of the study. Accordingly, the chapter contains a brief background to the study and then introduces the problem statement, the research objectives, the research methodology, delimitations of the study and ethical considerations. The theoretical background, which influenced the philosophical stance and methodological approach of the study, is also introduced in this chapter. In addition, the chapter contains a brief discussion of the key findings and, lastly, the thesis structure indicating the flow from chapter to chapter is explained.

1.1. Background

The National Small Business Amendment Act (26 of 2003) defines small and medium enterprises (SMEs) in accordance with the following five categories, namely, standard industrial sector and subsector classification, size of class, number of paid employees, turnover and asset value. However, for the purposes of this study an SME will be defined only in terms of the number of paid employees, namely, between 50 and 200. According to the Banking Association of South Africa (2017), SMEs have been identified as productive drivers of economic growth and development in South Africa. It is estimated that they make up 91% of formalised businesses, provide employment for approximately 60% of the labour force, while their total economic output accounts for approximately 34% of GDP.

The protection of their information assets against the complex and rapidly evolving security threat landscape is a major challenge for SMEs. The majority of such these concerns are associated with the leakage and modification of sensitive information, such as trade secrets, intellectual property and the interruption or destruction of critical ICT services (Webb, Ahmad, Maynard, & Shanks, 2014). According to PWC (2014), the average number of security incidents rose by 14% from 2011 to 2012 and by 20% from 2012 to 2013. Webb et al. (2014) attribute this rise to the increased use of social networking, the trend towards 'bring your own device' (BYOD) and the cloud computing technologies which are presenting new security vulnerabilities. These vulnerabilities are resulting in significant damage to the vital information asset and reputation of organisations and also have serious cost implications for these organisations (PricewaterhouseCoopers, 2015).

In 2015, PWC conducted a Global State of Information Security Survey which revealed that information security concern has shifted largely to the human element of information security. The survey found that 51% of the participants regarded insiders (current and former employees) as the likely source of incidents, while 46% of the participants cited outsiders (hackers and competitors) as the root cause of the

majority of information security incidents. Although the statistics are showing increased threats from the human element, the problem is also being aggravated by SMEs continuing to invest in technical controls such as antivirus and firewall technologies to protect information assets (Ifinedo, 2014; Pfleeger & Caputo, 2012). While an organisation may have a plethora of firewalls and antivirus systems in place, a naïve user may still usher in an attacker (Chipperfield & Furnell, 2010; Parsons, McCormac, Butavicius, & Ferguson, 2010). According to Colwill (2009), the 'employee factor' and technology together is the key to providing an adequate and appropriate level of security. Technology safeguards focus on digital data and not on the interaction between data and the employee, hence exposing the organisation's information assets to risk.

Although managers/owners of SMEs have been making significant efforts to implement policies and information security procedures to improve information security, the impact and effectiveness of these efforts remain questionable as the employees' non-compliance behaviours remain problematic (Goo, Yim, & Kim, 2014). Chipperfield and Furnell (2010) attribute this problem to a lack focus on proper employee awareness and training structures within the policies. Compliance with these policies requires awareness, an understanding of the policy itself and also how compliance applies to and helps the employees in their day-to-day activities. Schneier (2008) found that 62% of employees have limited information security knowledge while 38% are naïve. This helps to intensify the information security compliance issues.

The relevant literature agrees that a well-planned information security awareness campaign and training will alter the employees' behaviour in respect of compliance (Goo et al., 2014; Ifinedo, 2014; Otero, 2015; Pfleeger & Caputo, 2012; PricewaterhouseCoopers, 2015; Schneier, 2008). However, some SMEs still do not implement information security programmes, as it would appear that the generic, out-of-the-box solutions available on the market focus primarily on large organisations for

obvious profit-making reasons. This leaves SMEs exposed to security risks. In addition the SMEs often consider themselves too insignificant to attract threat actors, which is a dangerous misperception. Sophisticated adversaries are now also targeting naïve employees of SMEs as a means of gaining a foothold in the interconnected business ecosystems of the larger organisations with which the SMEs partner/sub-contract. This dangerous reality is compounded by the fact that larger organisations often make little effort to monitor the security of their partners, sub-contractors, suppliers, and supply chains (PricewaterhouseCoopers, 2015).

Employee security breaches may be costly to the organisation in several ways and may include lost productivity due to down time while the information systems are restored, monetary losses either directly or indirectly, disclosure of personal or sensitive corporate information, and a negative impact on the organisation's goodwill (Steele & Wargo, 2007). It is, thus, essential that employees understand how their intentional/non-intentional security breaches may significantly impact on the overall security position of the organisation (Colwill, 2009; Parsons, McCormac, Butavicius & Ferguson, 2014). According to Tamjidyamcholo, Baba, Shuib and Rohani (2014) and Ifinedo (2014), there is a strong and positive relationship between information security awareness and information security risky behaviour reduction expectations.

While the body of knowledge is growing in the area of information security policy drafting, implementation, awareness and compliance it would, however, appear that there have been few studies in the context of SMEs. In addition, there is a lack of compliance assessments models based on actual behaviours rather than on self-testified behavioural intentions. Lastly, there is also a lack of theories or models that may assist in motivating employee behavioural intention conversion into actual behaviours based on behavioural and deterrent theories.

1.2. Description of Problem Area

The effectiveness of information security awareness and training attempts to raise security compliance is still questionable, as some employees tend not to fully comply

with their organisation's security policies, regardless of the knowledge they have acquired through training (Shropshire, Warkentin, & Sharma, 2015; Siponen, Mahmood, & Pahnila, 2009). This may be attributed to two possible factors, namely, poor assessment methods that do not accurately measure the employees' knowledge and behaviours (Kruger & Kearney, 2005) and/or omissive behaviour (a gap in the employees' knowledge and behaviour) (Goo et al., 2014).

A survey conducted by Richardson (2008) found that 32% of the respondents do not measure information security policy compliance within their organisations. This is usually the result of the challenges involved in what to measure and how to measure it (Kruger & Kearney, 2005). Drafting an information security policy and implementing awareness campaigns/training do not automatically guarantee employee compliance. It is thus necessary to assess employee compliance (Kruger & Kearney, 2005).

According to Kruger and Kearney (2006), awareness initiatives are intended to increase knowledge, change behaviours and alter attitudes. However, the effectiveness of such drives is still uncertain as, regardless of their knowledge, some employees do not comply fully with their organisation's security policies (Shropshire et al., 2015; Siponen, Mahmood, & Pahnila, 2014). While academia generally suggests effective information security compliance practices within organisations, for example, Dhillon and Torkzadeh (2006) and Ma, Pearson and Tadisina (2005), industry practitioners, on the other hand, often report that employees' compliance with rules and security policies remains minimal. Goo et al. (2014) and Albrechtsen (2007) attribute this to employees perceiving security practices as interrupting their job routines. However, this study attributes this to the flaws in the assessment methods used as well as a lack of motivation in encouraging the conversion of intentions into behaviours.

1.2.1. Flaws in Assessment Mechanisms

Researchers (Allam, Flowerday, & Flowerday, 2014; Azjen, 1991; Ifinedo, 2014; Kruger & Kearney, 2006; Öğütçü, Testik, & Chouseinoglou, 2016; Safa & Von Solms, 2016) agree that in a perfect world, information security awareness should lead to

secure the behavioural intentions that should then lead to secure actual behaviour. These relationships are depicted in figure 1.

Figure 1.1: From awareness to actual behaviour

At the time of the study researchers assumed that assessing either employee awareness and/or their behavioural intentions equated to their actual behaviours. However, there is an undeniable gap between knowing and doing (Goo et al., 2014; Williams, 2009). Figure 1 shows two possible weak points, namely, Weak Point 1 and Weak Point 2. Weak Point 1 refers to a weakness in awareness failing to convert into positive behavioural intentions. This may be due to several reasons. For example, employees may perceive information security policies as general directives or mere optional guidelines, rather than seeing them as rules which must be followed (Goo et al., 2014). The majority of awareness assessment tools assess only employees' reception and retention of acquired knowledge and implicitly assume that such knowledge will infallibly lead to secure behavioural intention.

Weak Point 2 essentially shows the weakness of intention not infallibly converting into actual behaviour. Employees sometimes choose not to behave as they know they ought to behave as a result of factors that include lack of motivation, disagreement or cultural conflicts and interpretation of job routines (Albrechtsen, 2007). A traditional, intention based, information security assessment may reveal desirable (self-reported) behavioural intentions but leave actual insecure behaviours undetected (Greig, Renaud, & Flowerday, 2015). However, this may often be the result of social desirability bias while answering assessment questions (Krumpal, 2013).

An example from another practice serves to demonstrate the gap between knowing and doing. Hubbard (2002) quotes:

> It is believed that about 200 years ago people did not know about the germ theory; they did not know that they should wash their hands and boil surgical tools to limit the spread of disease and infection. Even though people know these things today, do they always wash their hands before eating, or even after doing something dirty?

Thus, even in 2016, achieving 100% hand-washing remains an intractable problem, even among those with the highest knowledge levels, namely, medical professionals (Brunetti et al., 2015; Bucher, Donovan, Ohman-Strickland, & McCoy, 2015). The research literature in a variety of areas on organisations illustrates the gap between awareness/knowledge and practice, for example in the areas of ethics (Schwitzgebel & Rust, 2014), smoking (Thrul, Bühler, & Herth, 2014), environmentally-friendly behaviour (Joshi & Rahman, 2015) and information security (Shaw, Chen, Harris, & Huang, 2009). It is, therefore, questionable whether any assessment based on knowledge, attitude and intention only would be sufficiently inclusive when assessing the success of information security drives or predicting actual behaviours.

1.2.2. Motivation for Conversion of Intentions into Actual Behaviours.

An employee who does not follow the information security policies, for whatever reason, constitutes the weakest link in information security, and this employee's omissive behaviour may seriously compromise the organisation's information security position. This highlights the need for alternative ways of motivating/enforcing the conversion of intentions into behaviour in attempting to achieve security compliance. For example, a vehicle driver has to learn the rules of the road and pass a driving test before obtaining a driving licence. However, this does not guarantee he/she will follow the rules and, thus, traffic police have to reinforce the traffic laws continuously, for example by traffic violation fines.

This above description of the research problem area reveals inconsistencies and gaps in the relevant literature. In order to simplify this complex phenomenon,

reconcile past findings and remedy existing current gaps, an action research study was undertaken in attempt to solve the problem discussed in the next section.

1.2.3. Statement of the Problem

Poor information security compliance within organisations is usually an indication of a lack of information security awareness (Hovav & Putri, 2016; Safa & Von Solms, 2016), which exposes employees to information security threats with the potential consequence of becoming the weak link in the overall organisational security initiatives (Burns, Posey, Roberts, & Lowry, 2017; Susanto & Chen, 2017; McLaughlin & Gogan, 2017; Safa & Maple, 2016). In addition, awareness initiatives do not necessarily result in safer employee information security behaviour because of the gap between knowing and doing (Goo et al., 2014; Park, Kim, & Park, 2017; Shropshire et al., 2015; Cox, 2012). This highlights the need for ways in which to reinforce compliance by ensuring the effective conversion of knowledge into intentions and intentions into actual behaviours (Han, Kim, & Kim, 2017).

1.3. Main Research Question

This research study aimed to address the problem of the conversion of behavioural intentions into actual behaviour that complies with the organisation's information security policy. The following primary research question was formulated:

How can SMEs in emerging economies reinforce employee information security policy compliance?

1.3.1. Sub-questions:

An extensive review of existing literature stimulated the formulation of the main and sub-research questions. Three sub-questions were derived from the themes of omissive behaviour, compliance reinforcement and information security compliance assessment as identified in the main research question (section 1.3.). Thus, the study addressed the following sub-questions:

i. **Is there a gap between employee behavioural intention and actual behaviours concerning the information security policy?**

An understanding of the gap between an employee's intention and actual behaviour is a vital foundation from which to adequately address organisational risk reduction. This sub-question categorised employee behavioural intentions and compared them to actual behaviours.

ii. **How should SMEs motivate or reinforce the conversion of behavioural intentions into actual behaviour?**

The first sub-question indicated a gap between employee behavioural intention and actual behaviours. This second sub-question intended to explore how this gap may be reduced by compliance reinforcement.

iii. **How should employee information security compliance be assessed taking into account the gap between intentions and actual behaviour?**

Finally, it was deemed essential to assess information security compliance to ensure the reinforcement initiatives have indeed resulted in changes to employee information security compliance. The intended output of this research study was seen as a solution in terms of which the gains would not gradually diminish over time.

1.4. Objective of Study

The primary aim of the study is to present a Framework for Information Security Compliance Reinforcement and Assessment. The reinforcement was through motivating or reinforcing the conversion of intentions into actual behaviour. Although there are numerous theories linking intention and behaviour, there are nevertheless some limitations in their relationship, namely, the intention–behaviour gap. This study sought to find new ways in which to reduce this gap and understand the mechanics of how behavioural intention converts to actual behaviour.

The employee assessment compliance model adapts and extends the Knowledge, Attitude and Behaviour (intention assessment) Model of Kruger and Kearney (2005) by means of the addition of two extra dimensions, namely, *competence* and *intention conversion* assessment. These dimensions were added in order to accommodate the gap between intention and behaviour.

The motivation/reinforcement for the intention to actual behaviour conversion model assists in explaining the role of awareness and how sanctions and rewards may assist in bridging the gap between intentions and actual behaviours with the end goal of facilitating information security compliance. Drawing on Deterrence Theory research in social psychology, it was possible to observe a relationship between penalties/rewards and behaviour and to derive suggestions of what the intention-behaviour association may hold either for employees fearing punishment or for employees attracted by the rewards associated with good behaviours.

The framework presented in this study was evaluated through expert review and tested and refined through an action research method approach using a sample of 30 employees and four iterations. The action research included employee information security awareness campaigns, online questionnaires (tests) and compliance assessments. This framework was intended to help to reduce the security gaps discussed in the earlier sections while also adding a different insight into the existing body of information security knowledge.

1.5. Significance of the Study

At the time of the study there was clearly a limitation in the existing information security body of knowledge in that it focused primarily on large organisations and "lacks insight or opportunities for SMEs" (PricewaterhouseCoopers, 2015). Several studies exploring information security awareness and training have been undertaken (McCormac, Zwaans, Parsons, Calic, Butavicius, & Pattinson, 2017; Bulgurcu et al. 2010; Talaei-Khoei, Solvoll, Ray, & Parameshwaran, 2011), as have information security compliance assessments (Cram, Proudfoot, & D'Arcy, 2017; Kruger &

Kearney, 2006; Hwang, Kim, Kim & Kim, 2017; Parsons et al., 2017; Da Veiga & Eloff, 2010; Vroom & Von Solms, 2004). However, the issue of the gap between the knowledge acquired from awareness and training and compliance with policies within SMEs remains relatively unexplored. Compared to larger organisations SMEs are more vulnerable to information security threats because intruders are using them as a pathway to the larger organisations that usually outsource to these SMEs for projects (PricewaterhouseCoopers, 2015). However, unlike larger organisations, they have limited resources to recover should a security breach occur.

When an organisation is working towards cultivating compliance there is a need to assess whether the goal is being achieved. In many areas of psychology if something cannot be measured it cannot be studied. The same is true for information security compliance. For example, no one would embark on a realistic diet/exercise plan without any means with which to monitor either its success or its failure. Information security compliance involves an employee's behaviours and these are difficult to measure because there is no agreed framework of what to assess, or how to assess it (Kruger, Drevin, Steyn, 2010). Organisations could thus benefit from guidance in establishing information security compliance assessment initiatives which may then be subsequently refined and improved to maximise compliance by cultivating applied security knowledge. In addition, assessment also helps in motivating/reinforcing compliance. According to ENISA (2007) many organisational leaders agree that "what gets measured gets done".

Accordingly, in response to the gap revealed in the literature, this study developed a framework for assisting in closing this gap by motivating/reinforcing the conversion of knowledge into sound security practices and assessing information security compliance. The model counteracts the main causes of behavioural intents which do not translate into actual behaviours. The framework presented not only provides an outline and insight to help SMEs to design and implement an information security compliance assessment tool, but also helps in forecasting the information security

compliance profiles of employees. These compliance profiles should provide an indication of the employee information security culture as it manifests in behaviour.

In short, this study developed, refined, validated and presented an Information Security Policy Compliance Reinforcement and Assessment Framework. Such developments are a useful addition to the existing body of knowledge in the field of information security, as they constitute an initiative for moving towards the establishment of the standardisation lacking in this field. This framework developed in this study may be adapted for use by other, similar SMEs.

1.6. Initial Review of Related Literature

According to Hofstee (2006) literature review is meant to give the researcher a better understanding of the research problem, provide a theoretical base of work still to be done and lastly position the proposed research with research that has already been done. This study conducted a thorough review of a variety of literature, notably books, journal papers, conference papers, white papers, theses, articles and websites. During the literature review the theoretical foundation of the study was discussed first, after which all the other related research articles were briefly discussed.

1.6.1. Theoretical Foundation

An increasing number of information security researchers have begun to adopt an instrumental view of employee compliance, drawing upon a variety of theories including the Deterrence Theory (DT) (D'Arcy & Herath, 2011; Herath & Rao, 2009); Control Theory (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009); Theory of Planned Behaviour (TPB) (Bulgurcu, Cavusoglu, & Benbasat, 2010; Dinev et al., 2007); institutional theory (Hovav, 2017; Kshetri, 2013; communication theory (Johnston & Warkentin, 2010); learning theories (Puhakainen & Siponen, 2010) and criminology theories (Siponen & Vance, 2010; Willison & Backhouse, 2006). These studies have all provided insights about the way in which a variety of organisational efforts may enhance employee conformity with security policies.

However, for the purposes of this study three behavioural theories were used, namely, Theory of Planned Behaviour (TPB) (Bulgurcu, 2010), knowledge, attitude, behaviour (KAB) theory (Kruger & Kearney, 2006), and Deterrence Theory (DT) (Hovav, 2017). These were specifically selected because their constructs adequately explain human behaviour.

1.6.2. Preliminary Review of other Empirical Studies

Recent studies on data breaches have indicated that employees are the cause of many of the breaches that occur, whether intentionally or unintentionally (Furnell & Thomson, 2009; Gundu & Flowerday, 2013; Kruger & Kearney, 2008; PricewaterhouseCoopers, 2015). These studies concluded that organisations should pay serious attention to reducing the risk that employee behaviour constitutes with research emphasising that the behaviour of employees should be moderated to ensure that it secures the information assets (Albrechtsen, 2007; Cox, 2012; Kraemer & Carayon, 2007; Kruger & Kearney, 2008; Brewer, 2013; Stanton, Stam, Mastrangelo & Jolton, 2005; Van Niekerk & Von Solms, 2010). When attempting to reduce both intentional and unintentional data breaches caused by employees, a trusted technical infrastructure, awareness campaigns, good corporate governance, and other security measures are among the aspects which need to be addressed (Da Veiga & Eloff, 2010; Ifinedo, 2012).

Employees are often perceived to be the weakest link in the information security chain and, hence, it is vital that this weak link is strengthened. Educating employees and increasing employee awareness of the expected security behaviours and how to respond to security incidents based on the organisation's information security policy represent an attempt to overcome this 'weakness' (Allam et al., 2014; Stephanou & Dagada, 2006; Pfleeger & Caputo, 2012 Safa & Von Solms, 2016; Schneier, 2000; Van Niekerk & Von Solms, 2004). The best information security policy and procedures are ineffective if there is no implementation of an information security awareness programme, or the awareness programme implemented is not effective

(Russell, 2002) because the existence and contents of the organisation's information security policy may be unknown to its employees.

The effectiveness of attempts by SMEs to raise security awareness is questionable as practitioners have continuously reported that the issue of poor employee compliance with information security policy prevails. This despite the fact that awareness campaigns have been actioned and an effective security policy exists (Goo et al., 2014; Siponen, Mahmood, & Pahnila, 2009; Vroom & Von Solms 2004). This emphasises the need for alternative ways of reinforcing security compliance.

The majority of the information security assessment studies which have been conducted tend to focus on behavioural intentions as a predictor of actual behaviours. However, significant recent studies have also pointed out that intentions are not infallible predictors of behaviours. Ajzen (1985) suggests that some are abandoned altogether while some are revised to meet changing circumstances due to unforeseen events. He also posits that intentions change over time – the greater the time period, the greater the chances of unseen events which may lead to intention changes.

Psychologists Ouellette and Wood (1998) are of the opinion that past behaviours guide future behaviours. They suggest that well-practised behaviours reoccur because they have become part of the employees' culture and, alternately, when behaviours are not well learnt, employees tend to be more conscious when making decisions to initiate and carry out such behaviour. Hence past behaviour, attitudes and subjective norms will inform new behaviours. It is widely agreed that these relations between past behaviour and future behaviour have been substantiated. However, in terms of information security compliance assessment, past behaviours only after awareness and training initiatives should be measured as, otherwise, the security state and behaviour prediction will probably be inaccurate.

Payne (2010) acknowledges the difficulty involved in assessing information security compliance and proposes using metrics. The metrics use a top-down approach that starts with the objectives of the security programme and then works backward, identifying specific metrics that assist to determine whether these objectives are being realised before finally proposing measurements to generate these metrics. For example, firstly, defining/listing the objectives of the overall security programme, secondly, identifying metrics that would indicate progress toward each objective and then, lastly, determining the measurements required for each metric. This study adopts the following stance, namely, the metrics method does not solve the problem because it does not assist with identifying those metrics that will indicate progress.

Kruger and Kearney (2006) identified two distinctive challenges in developing a measuring tool, namely, what to measure and how to measure it. They, however, decided to measure three dimensions, namely, *knowledge* (what you know), *attitude* (what you think) and *behaviour* (what you do). Each of these dimensions is then subdivided into focus areas. Where appropriate, these focus areas would then be further subdivided into specific factors.

The reality that standardisation is an ongoing problem is made by clear by recent studies still not adopting a standard way of carrying out information compliance assessment. Safa, Von Solms, and Furnell (2016) view possible constructs of information security compliance as involvement, attachment, commitment and personal norms while Posey, Roberts, Lowry, and Hightower (2016) argue that they are wary of sanctions, incentives, motivations and pride as possible constructs.

Although organisations adopt and employ different information security assessment methods, a paucity of empirical studies on information security assessment models that assess actual behaviours is evident. The majority of studies still assess behavioural intention only despite the acknowledgement that intentions do not reliably convert into actual behaviour. The main reason for this is that it is challenging to assess actual behaviours and, in the main, the behavioural intention is deemed to be a “good enough” proxy. Nevertheless, the literature reveals that these

assessments are also highly recommended and should be carried out periodically so as to also monitor changes in security trends.

The literature review conducted in this study showed that, in an effort to enforce policy and to ensure the compliance of insiders, security managers often utilise a variety of techniques, including security education, training, awareness programmes, events, incentive programmes and campaigns. Unfortunately, the degree to which an individual perceives information assets as personally relevant is highly subjective and this potentially marginalises the impact of the fear appeal. These threats, while very real, are not universally personally relevant (Johnston, Warkentin, & Siponen, 2015). In addition, the literature review also revealed the absence of studies on compliance motivation/reinforcement techniques and compliance assessment techniques that assess actual behaviours and not only behavioural intentions on the basis of psychological/behavioural theories.

1.7. Research Design and Methodology

Research methodology refers to the process of systematically solving the research problem. It may, thus, be regarded as a process of learning how research is conducted scientifically. Thus, the various steps adopted by a researcher in studying the research problem together with the logic these steps are investigated (Collis & Hussey, 2009; Hofstee, 2006). The research paradigm that provides insight into the beliefs, values and techniques which were relevant to this study are discussed below.

1.7.1. Research Paradigm

There are several paradigms that exist and which may be distinguished by the philosophical assumptions on which they are based. This section briefly discusses the research paradigm used for this study. According to Collis and Hussey (2009), positivistic and phenomenological paradigms are two extremes and only a few of these paradigms would operate in their pure forms. Figure 1.3 depicts the difference between the positivistic and the phenomenologist approach.

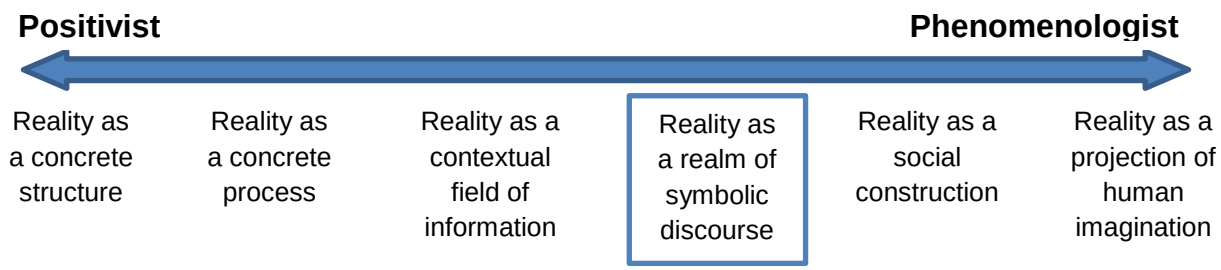


Figure 1.2: Continuum of core ontological assumption (Morgan & Smircich, 1980, in Collis & Hussey, 2009)

This research project focused on cultivating security compliance by changing employee behaviours. Thus, an action research approach with an interpretivist bias in line with the reality as a realm of symbolic discourse section of the continuum, as represented in Figure 1.3 was adopted. This section of the continuum views the social world as a pattern of symbolic relationships which are sustained through a process of human action and interaction (Morgan & Smircich, 1980, in Collis & Hussey, 2009). The approach used in this study was based on inductive reasoning. In other words, the researcher formulated the research questions and then conducted observations and surveys from which general conclusions were drawn based on the employee behavioural trends identified.

1.7.2. Research Method

Research methods refer to the techniques used to acquiring the requisite knowledge. These methods are often divided into two main types, namely, quantitative and qualitative research methods (Muijs, 2011). Qualitative data are usually text based (Rossman & Rallis, 2003) while quantitative data comprise numerical data (Muijs, 2011).

Although this study primarily adopted an interpretivist approach which uses inductive reasoning in which theory is derived from empirical data, the study also used a quantitative research approach for the purposes of data collection and data analysis. The quantitative approach seeks to control and predict while qualitative research focuses on description, analysis and interpretation. This study used a combination of qualitative and quantitative data collection techniques (mixed methods) in parallel although the qualitative data collection and analysis methods were prioritised

1.7.3. Research Design

The research design is a plan of action which guides the research process from the research questions to the actual implementation. As such, it provides the detail on the way in which the data will be collected and analysed (Terreblanche, Durrheim, & Painter, 2006). In order to carry out a comprehensive study of the research subject matter, an action research design was chosen.

There are several forms of action research. The most prominent in the information system context include participatory action research and canonical action research. The key difference between these two is the researcher's role in the study. In participatory action research the researcher is both a participant and researcher. However, in canonical action research, the researcher intervenes from an outsider perspective (Davison, Martinsons, & Kock, 2004). For the purposes of this study the researcher conducted canonical action research at a civil engineering consulting organisation based in East London (South Africa). The organisation is heavily dependent on information systems and there are vast amounts of information which consists mainly of sensitive intellectual property (engineering designs, as-builts and GIS data) stored on the servers. The organisation has almost all the typical characteristics of an engineering SME in an emerging economy.

The researcher was actively involved with the employees at the organisation. The study was a cyclical process that linked theory and practice. The framework presented in Chapter 7 was validated through expert review and was refined after every cycle of the action research. The action research took the form of a field intervention that aimed at solving the practical, real information security problems faced by engineering SMEs in emerging economies. This approach was in line with Baskerville's (1999) view that action research is ideal for studying information system methods in a practical setting and empirically studying the applicability of proposed new solutions in practice and, possibly, their refinement.

The study included empirical research as well as an intensive literature review which is briefed in the next section.

1.7.2.1. Data Collection

Data collection techniques enable the systematic gathering of information about the objects of study and about the settings in which they occur (Collis & Hussey, 2009). This research study collected both primary and secondary data in accordance with the cycles of the intervention and the nature of the information required. Secondary data was mostly from books, journal papers, conference papers, white papers, theses, articles and websites. All attempts were made to keep the content as current as possible as these sources formed the theoretical foundation of the study.

The research was undertaken in cycles to enable the framework to be refined as well as to evaluate whether compliance was improving after each information security initiative and primary data was collected in each iteration. The primary data was collected by the use of web based questionnaire/survey tests, observations and informal interviews. The data gathered from the informal interviews and observations was then used to analyse actual behaviours and to determine existing knowledge gaps for awareness and training purposes. The data from the online surveys was used to assess behavioural intentions. Secondary data was collected from published articles, books, the internet and relevant dissertations.

1.7.2.2. Data Analysis

Information security compliance behavioural patterns were then identified and categorised adapting the similar processes Lichtman's (2013). The data which had been collected was weighted according to an importance scale agreed upon by the researcher and the organisation's management. All the questions in the survey were structured in a way that extracted data on the phenomenon being assessed. Data analysis was conducted after each iteration and then compared to the results of the subsequent iteration in order to assess changes in the employees' compliance with information security.

1.8. Delimitation of the Study

The drafting of an information security policy is the first step that an organisation should take to secure its information asset. However, this was beyond the scope of this study and in fact the organisation already had a comprehensive information security policy in place. There are two types of insider/employee threats, namely, naïve mistakes and intentional security breaches on the part of disgruntled employees seeking revenge. This study focused only on the naïve mistakes made by naïve employees, although the literature shows that disgruntled employees may also pose a serious security risk.

Although this study and others by Shropshire et al. (2015) and Ngoqo and Flowerday (2015) emphasise that the behaviour of employees should be addressed in order to protect information assets, the most effective countermeasure is to implement a variety of controls and not just behavioural measures. Such other security measures that should be considered when aiming to reduce both the intentional and unintentional damage caused by employees and that were not part of this study include, but are not limited to, a trusted technical infrastructure, reliable internal processes and good corporate governance.

1.9. Ethical considerations

This study complied with the ethical policy as set out by the University of Fort Hare Ethics Committee. It was, therefore, the responsibility of the researcher to ensure that their participation in this research study would not expose the employees who took part in the study to any negative consequences. In order to ensure beneficence, both informed consent and the principles of anonymity were applied to the study. No identifiable information about the employees was revealed in publications. Furthermore the respondents were informed of both the voluntary nature of their participation as well as their right to withdraw from the study at any point if they felt uncomfortable.

1.10. Main Findings of This Study

The literature review revealed that the human factor is often underrated or underplayed in the securing of information assets. It is, however, crucial to ensure that employees act and behave in a secure way. As this study revealed that merely furnishing people with knowledge and know-how will not achieve this, as such knowledge and know-how are essential, they are not sufficient to guarantee compliance. Assessing actual compliance is crucial if areas of non-compliance are to be highlighted in order to identify those areas which require more focused attention. Moreover, such assessments provide evidence of the competence-driven value which may be used to justify the resources used in such drives.

Expert reviews concluded that the framework presented in the study was well structured, could be easily followed, was of high technical quality, was unique and very comprehensive, it added new knowledge to the field of information security and it had a originality.

The proposed framework was tested in practice through an action research process which comprised four iterations. The first iteration revealed that the employees possessed very little or no information security knowledge. An information security awareness campaign was then carried out to address this lack of knowledge. The second iteration revealed an increase in the information security knowledge but still revealed some gaps in other aspects of security. These were then addressed by another awareness campaign. It was discovered after the third iteration that although the employees had become more aware of security behaviour and had indicated positive behavioural intentions, these had not materialise into actual positive behaviours. This revealed a gap between ‘knowing and doing’. This gap was then addressed by reinforcing compliance by introducing rewards for secure behaviours and punishments for unsecure behaviours. The assessment tool used was then also modified to measure not only behavioural intentions but also to assess actual behaviours. This was done because the tool had provided an inaccurate information

security picture as behavioural intentions do not always equal actual behaviours due to psychological factors that were beyond the scope of this study.

1.11. Structure of Thesis

This thesis is divided into eleven chapters.

Chapter 1 is an introductory chapter and includes a discussion of the background to the study, the identification of the research problem, an outline of the research objectives and a brief discussion of the research methodology used.

Chapters 2 through to 5 present of the literature study (secondary research) and discuss existing literature available on insider threat, the knowing and doing gap, awareness campaigns and information security compliance, its reinforcement and its assessment.

Chapter 6 discusses the design and development of the proposed framework (information security policy compliance reinforcement and assessment framework) and its theoretical foundation.

Chapter 7 discusses the research design and research methodology used and includes the data collection and data analysis techniques used in the study.

Chapter 8 discusses the empirical exploration undertaken and describes the action research intervention that was conducted then outlines the research findings from the action research intervention.

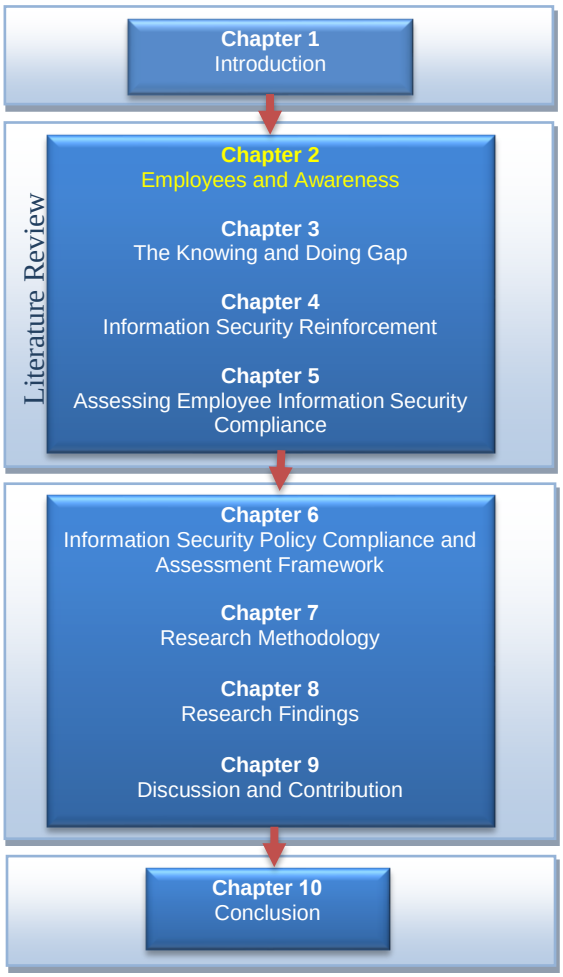
Chapter 9 presents the discussion and outlines the contributions of the study as well as recommendations for SMEs in emerging economies as based on the findings.

Chapter 10 contains a summative conclusion that determines whether the research study addressed the research problems and indicates any problems that may require further research.

1.12. Chapter Overview

This study was conceived against the backdrop of efforts made by SMEs to protect their information assets. The study also highlighted the risky nature of the naïve employee. This chapter attempted to summarise all the activities undertaken during the study. It then briefly explained the information security policy compliance reinforcement and assessment framework that may be adapted to minimise employees' negative security behaviours. The framework introduced was based on three behavioural theories, namely, TPB, KAB theory and DT. This chapter also summarised how the information security policy compliance reinforcement and assessment framework had been validated and refined.

CHAPTER 2 - EMPLOYEES AND AWARENESS



Chapter 2:

The discussion in this chapter aimed at providing a comprehensive understanding of the insider (employee) in terms of information security risk. This was followed by an overview of the ways in which the risk they pose may be mitigated. Global insider statistics at the time of the study were then explored and, finally, information security awareness is introduced as a way in which to mitigate this risk.

2.1. Introduction

The ICT use of SMEs relies heavily on the information stored on servers and communication over networks/internet. The information stored on the computer systems often includes both unpatented and patented private and confidential designs, client and employee databases and, in some cases, trade secrets. However, this sensitive information is vulnerable to both external and internal threats. The increase in connectivity and resource sharing has led to an increase in the likelihood of external threats which may result in data theft, defacement, commercial espionage from competitors or bad wishers and other forms of loss of the organisation's important information. However, internally, there is an even bigger threat posed by the insecure behaviours of naïve insiders (employees) not behaving in a secure way.

However, several engineering SMEs tend to be more concerned about their vulnerability to external threats as compared to their vulnerability to internal threats despite the fact that industry-specific research suggests that a substantial proportion of security incidents originate from inside the organisation (Al Hogail, 2015; Etsebeth, 2006; Furnell, 2006; PricewaterhouseCoopers, 2015; Sarkar, 2010; Stanton et al., 2005).

The challenge for organisations is to ensure awareness of their security policies and procedures to their employees are trained on how to implement them in their daily routines in consistent manner. Technical security controls assists in reducing the threat of malicious employees. However, the defence against naïve employees lacking understanding necessary to safeguard information may be achieved by vigorous security awareness and training programme. The hour it takes an employee to view an awareness presentation may be the difference between a secure organisation and a multimillion Rand breach of security. This chapter starts by defining the insider and then discusses the risk to which the insider may expose the organisation. This is followed by a review of insider risk statistics at the time of the study.

The chapter identified employee classifications and assessed risks to which they may expose their organisations. The multi-user era, which has been brought on new technologies that allow computers to multi-process and log on multiple users concurrently, has led to a high degree of organisational dependency on information and communication technology (ICT). Such ICT is usually used for internal operations such as record-keeping, emails, VoIP, banking, and online-marketing.

2.2. The Employee (Insider)

For the purposes of this research study, insiders and outsiders are distinguished by the definitions below:

- **Insider**: Current or former employee, service provider or contractor.
- **Outsider**: An individual who has never had authorised access to the organisation's systems or networks.

The insider usually has unregulated access to some part or else parts of the information system. According to Wood (2000), one or more of the following assertions are assumed to be true about an insider:

• The insider breaches are from within the system's perimeter defences.

• The insider breach will not trigger the perimeter defences alarm hence will not arouse the network security personnel.

• The insider has physical access and rights to the system that compromises the system's perimeter network defences.

On the other hand, outside attackers attempt to gains access to the inside of a network either by attacking the system directly or by exploiting the weaknesses of an employee. This research study focused on insiders only. The reason for this segregation was that the insider threat is usually taken for granted and organisations often have limited systems in place to minimise the risk to which insiders expose the organisation as compared to that posed by outsiders with firewalls and physical security being used to guard against intruders.

2.2.1. Corporate Citizenship of Insiders

According to Sarkar (2010), insiders may be divided into pure insiders, insider associates and inside affiliates. The pure insider and associated insider are discussed briefly in figure 2.1. The affiliates are self-explanatory.

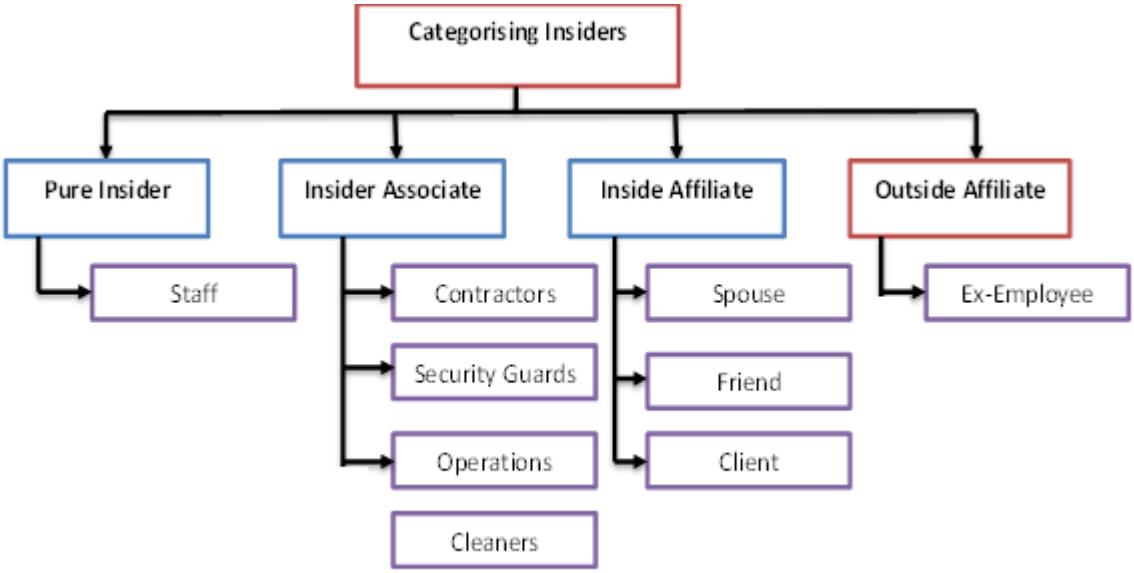


Figure 2.1: Categorising Insiders (adapted from Sarkar, 2010)

2.2.1.1. Pure Insider

Pure insiders are full-time and part-time employees with the required privileges, such as keys, access cards and the network logon, to enable them to perform their job functions (Sarkar, 2010). Employees pose the greatest risk to the organisation in terms of access and potential damage to sensitive and private information systems. As members of the organisation who have been vetted employees are trusted and are expected to have an interest in the productivity and success of the organisation. After their recruitment employees are considered as “members of the family” and are, therefore, often above suspicion. This means that they are often the last to be suspected when systems malfunction or fail (Shaw, Ruby, & Post, 1998).

In addition, some form employees still have rights to the organistaional information asset. This qualifies them still as insiders. Employees may anticipate termination of their contracts and prepare backdoor access beforehand or simply loot organisational information for later use. There are a number of recorded cases in which disgruntled

former employees have returned to seek revenge. This calls for the need to improve the management of employee termination. (Shaaw et al., 1998).

2.2.1.2. Insider Associate

Insider associates are usually third party employees such as contractors, partners, consultants cleaners, security guards and temps, or suppliers. These usually have limited/restricted access on the networks. However they may have access to employees' desks, rubbish bins who may be naïve to leave sensitive information such as usernames and passwords under keyboards, stuck on monitors. The more sophisticated ones may even plant key loggers on the non-suspecting pure insiders' computers.

Insider associates are separated from pure insiders because often their screening and background checks are less vigorous as compared to pure insiders. Most organisations have little or no control over a contractors or consultants hiring procedure. These often end up having highly privileged access to the organisation's information assets (Shaaw et al., 1998).

2.2.2. Attributes of the Insider

A variety of attributes may be used to describe the insider. These attributes include, but are not limited, to access, knowledge/skills, risk and process.

2.2.2.1. Access

Resources, such as storage and databases, are often shared and may be accessed remotely in a distributed fashion. This has given rise to the problem of ensuring that authorised users only gain access to these resources. It is for this reason that technical controls, such as authentication and access controls, are being implemented (Du Plessis, 2002).

2.2.2.2. Knowledge/Skill

Organisations often comprise various departments. The employees in these departments tend to have different levels of knowledge, experience and skill. It should, therefore, be taken into account that these employees will have different

backgrounds in terms of their knowledge and skill in respect of information security. It would, thus, not be accurate to conclude that they will behave in the same manner so regards ensuring that the organisation's assets are secure (Pfleeger & Caputo, 2012).

2.2.2.3. Risk

The insider is very risk-averse. The risks to which the employees expose the organisation is not the same as these risks depend on the levels of information security awareness of the particular employees as well as the type of information to which they have access (Colwill, 2009).

2.2.3. Motivation behind Attacks

The motives behind attacks on the organisation's information assets include unintentional insecurity/naïve mistakes and also intentional insecurity/dangerous tinkering. Figure 2.2 summarises the motives behind these attacks.

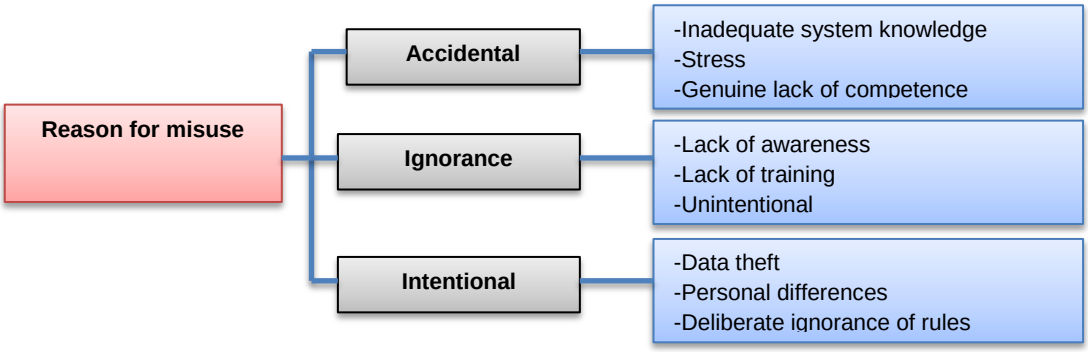


Figure 2.2: Reasons for Misuse (Magklaras & Furnell, 2001)

2.2.3.1. Unintentional Insecurity/Naïve Mistakes

These mistakes can either be accidental or out of ignorance. A few examples of costly naïve mistakes are discussed below. It must, however, be noted that these examples represent just a small percentage of the security breaches which may occur because of the lack of an established security awareness programme:

Example 1: Snapchat fell prey to a whaling attack back in late February 2016. According to the Washington Post, a social engineer with criminal intent posed as CEO Evan Spiegel and sent an email to someone in the social network's payroll

department. As a result, the personal protected info (PPI) of some 700 employees was released.

Snapchat published a company blog post stating they were "just impossibly sorry" for the breach and taking appropriate action with the FBI and other investigative bodies (Washington Post, 2016).

Example 2: Whitehead Nursing Home in Northern Ireland was recently fined some 15,000 pounds by the Information Commissioner's Office (ICO) for negligence in a data breach, according to the BBC News. An employee took home an unencrypted work laptop, which was stolen later in a home burglary. The news story states that protected data on 46 employees and 29 patients was exposed (BBC news, 2016).

Example 3: An East London hospital complex employee made the server with the patients' details accessible on the internet. Detailed personal information (names, contact details of their next of kin, ID numbers, dates of birth, telephone numbers, home addresses, marital statuses and occupations) of patients who had been to Hospitals was disclosed. This was in breach of the Patient Rights Charter to which all hospitals subscribe to (Med-e-News, 2010).

Example 4: An ebay online retailer experienced the biggest yet reported breach by an online retailer (PC World, 2015). Attackers compromised a "small number of employee log-in credentials" during the last week of February and first week of March 2014 and used them to gain access to the company's network to compromise a database that contained personal customer details (names, email addresses, physical addresses, telephone numbers, encrypted passwords and dates of birth). The breach affected the more than 100 million of their 145 million members. All members were then requested to change their passwords. This breach occurred through social engineering to unsuspecting employees (PC World, 2015).

These examples were **not** the acts of a malicious insider (employee) attempting to seek revenge, discredit the organisation or make profit through industrial espionage. Each situation involved a naive employee who lacked proper training or awareness necessary to behave securely. Awareness and training would have avoided the negative impact caused to these organisations goodwill.

2.2.3.2. Intentional Insecurity/Dangerous Tinkering

Employees who intentionally cause damage through the abuse of organisational trust. They use their legitimate access to information resources for illegitimate purposes. According to Sarkar (2010) the motives for the insecurities are as shown in Figure 2.3.

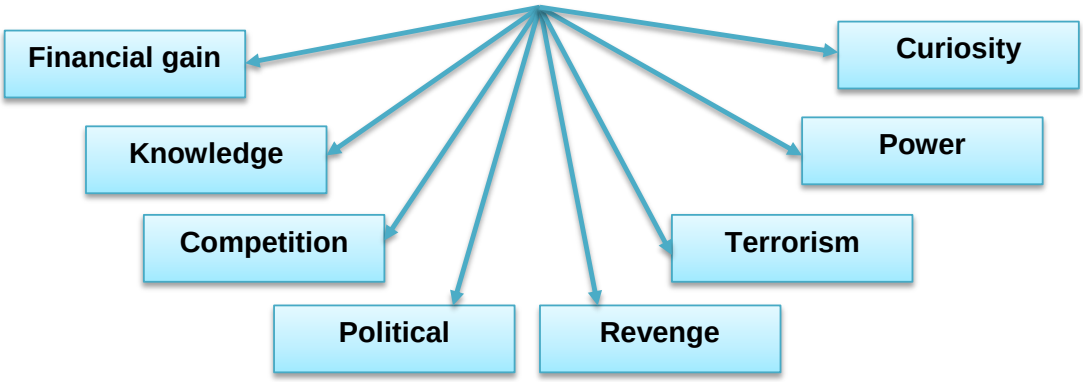


Figure 2.3: Components of the Motivation behind Intentional Damage (Sarkar, 2010)

The organisation may employ individuals who exhibit narcissistic traits. These individuals are often identified as the office bully, a toxic manager or an arrogant prima-donna. However, such individuals may present risks to the organisational information security. These personality types tend to engage in risky behaviour such as denial, rationalisation and impulsive actions, and often demonstrate a sense of entitlement. Just as narcissism applies to individuals, so may narcissistic personality behaviour occur at the organisational level (Brown, 1997). Both the narcissistic individual and the narcissistic organisation develop identities that are reflected in their policies, procedures, behaviours, values and beliefs and these have an impact on the intentions and actions of the employees. These individuals and organisations tend to be self-absorbed, they feel self-important, they are obsessed with success and

power, they lack empathy and they exploit others (Duchon & Burns, 2008). Corporations such as Enron and, more recently, the General Services Administration at their Las Vegas convention, are prime examples of organisational narcissism.

The four case examples below contain incidences of intentional insecurity:

Example 1: An ex-Ford engineer was charged with stealing sensitive design documents worth millions of dollars from the automaker and then trying to use them to find a job at a competitor automaker in Beijing (Computerworld, 2009).

Example 2: Two former Coca-Cola employees were sentenced to federal prison terms for conspiring to steal and sell trade secrets to rival Pepsi for $1.5 million. Joya Williams, 42, of Norcross received an eight-year prison term while Ibrahim Dimson, 31, received a five-year term according to a news release from the US attorney's office for the Northern District of Georgia. Both were ordered to pay $40 000 in restitution (CNN, 2007).

Example 3: A 32-year old employee of UK-based payroll company Sage deliberately committed data theft with presumed intent of fraud according to a recent report by Fortune. The suspect was recently arrested at London's Heathrow Airport. The news story states that stolen data included bank account information and salaries. At the time of writing, no reports of insider-outsider collusion have been released, indicating it could be a true single-actor incident (CNN, 2015).

Example 4: A disgruntled employee exposed the protected details of India's new Scorpene submarines in a complex data breach that involved multiple governments, employees, and contractors. According to Defense News, some 24,000 pages of classified information were exposed. The news story relates that a terminated employee chose to copy data to a disk, mail it, and eventually share it with a journalist (Defence News, 2016).

Example 5: A former financial adviser at Variable Annuity Life Insurance was found in possession of a USB drive that contained details of 774 723 of the company's customers. The drive was returned to the company by law enforcement officers as the result of a search warrant served on the former adviser. The USB drive included full or partial social security numbers. However, the insurance company stated that it did not believe that any of the data had been used to access customer accounts (PCWorld, 2014).

2.3. The Risk Posed by the Employee with Respect to Information Systems

Risk refers to "the likelihood that a threat materialises" (Stoneburner et al., 2002). To some degree risk is unavoidable and organisations have to accept a degree of risk. Elky (2004) maintains that risk is not caused by humans only, and identifies the following common threat sources:

- **Natural threats**: floods, earthquakes, hurricanes
- **Human threats**: threats caused by human beings, including both unintentional (inadvertent data entry) and deliberate actions (network based attacks, virus infection, unauthorised access)
- **Environmental threats**: power failure, pollution, chemicals, water damage.

Risk may be perceived as the probability of loss or damage. According to the US DOD (1999), risk management is a function of three variables, namely, criticality, vulnerability and threat. The first element of criticality refers to 'How important is this asset to the organisation?' while the second element of vulnerability refers to 'In what ways can the asset be compromised, exploited, damaged or destroyed?' The third element of threat refers to 'Who intends to exploit vulnerability, against what, and what capabilities do they possess to do so?' Risk occurs at the intersection of criticality, vulnerability and threat (US DOD, 1999). Figure 2.4 below illustrates the intersection of vulnerability, threat and criticality which forms risk.

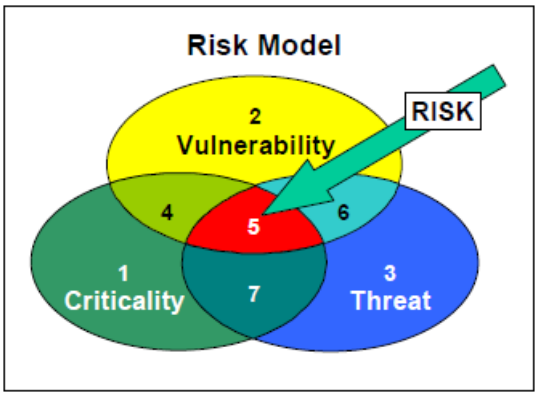


Figure 2.4: The Risk Model (US DOD, 1999)

Risk management involves understanding the value of information to the organisation and others and the putting in place of protective measures which are in line with the value of the information (US DOD, 1999). Any response must be appropriate to the threat posed, for example, locking and dead bolting a window to keep the rain out when simply shutting the window would have the same effect. Response is also linked to the timeliness of the action taken, for example, shutting the window after the rain has stopped and has already come in the window is too late. With the increasing interconnectedness of systems, it is important a rapid response is essential to contain the threat and limit further damage.

2.3.1. Why Manage Security Risk?

In today's highly networked systems environment, it is often very difficult for organisations to protect the integrity, confidentiality, and availability of their information without ensuring that each employee involved shares the same security vision of the organisation, understands their roles and responsibilities, and is adequately trained to perform these roles and responsibilities (ISO 27002, 2013). In order to assist in ensuring information security, individual users require knowledge on their specific role in the security process. This knowledge may be provided via education, training and awareness campaigns (Van Niekerk & Von Solms, 2010).

Employees may expose organisations to several risks, for example the unintentional leaking of confidential information when attacked by social engineers who targets and convince employees to unintentionally engage in risky behaviour. Social engineers are experts at appealing to the employees' emotions in order to

fraudulently obtain sensitive and private information. They persuade employees by manipulating and exploiting fear, trust, the desire to be helpful, or the urge to simply cut corners and save effort (Workman, 2007).

In many instances users simply do not understand the rules or the rationale behind the relevant policies, or they do not recognise the threat to the organisation's information assets and the risk involved in ignoring proper procedures. Not following simple procedures such as choosing a strong password to secure confidential information, is an example of not understanding the reasoning behind the rule (Zviran & Haga, 1999).

The following answer to the question 'Why should SMEs consider managing information security risk?' is found in the literature: namely, because it matters to the customers/clients, investors, employees and trading partners of the SMEs. It is vital that an organisation safeguards its trade secrets, protects privacy, and maintains its reputation.

2.3.1.1. Trade Secrets and Know-how

Trade secrets are the catalysts that have either spawned new types of businesses or enabled businesses to remain afloat by creating new ways in which businesses may outperform their rivals (Porter & Millar, 1985). Thus, trade secrets are a special type of intangible asset that gives a company a competitive advantage. Know-how is one of the most common types of knowledge which is protected as a trade secret and it defined as the unique knowledge of how something is done. Trade secrets can include formulae, inventions, programs, methods, techniques and processes. Unlike other types of intellectual property, such as copyrights and patents, trade secrets are protected by preventing them against becoming known.

Know-how is deemed to be a trade secret only if it is truly a secret, it has economic value and it is properly protected. For a company to remain competitive it must carefully control who has access to its trade secrets. Certain authorised individuals require access to such information in order to be able to use it for the company's best

interest. However, if unauthorised individuals gain access to such information it can jeopardise the company's competitive advantage.

2.3.1.2. Confidentiality

In addition to trade secrets, it is incumbent on a company to safeguard the personal information given to it by its customers. Generally, when a customer shares his/her private information with a company, this is only in exchange for a good or service from the company. For example, consider the extensive medical information a patient must give to a surgeon. Although most patients are reluctant to provide this information they will usually do so willingly when they require surgery and when they trust the healthcare provider (Hartman, 2012).

2.3.1.3. Branding, Reputation, and Customer Trust

Seth Godin, a highly respected blogger and author of 17 books, defines a brand as "the set of expectations, memories, stories and relationships that, taken together, account for a consumer's decision to choose one product or service over another. If the consumer (whether it's a business, a buyer, a voter or a donor) doesn't pay a premium, make a selection, or spread the word, then no brand value exists for that consumer" (Godin, 2009).

A powerful brand conveys a promise to its customers that a company then keeps consistently over time (Odoom, Agbemabiese, Anning-Dorson & Mensah, 2017). Trust is very closely linked to the persistent keeping of a promise and the building of a reputation for being trustworthy (Bidmon, 2017).

Businesses spend vast amounts of money building their brands in order to differentiate their products and services (Van den Driest & Weed, 2014). Nevertheless, certain companies have incurred significant damage to their brand and company reputation because of data security breaches which have resulted in the loss of sizable amounts of money as customers shift to competitors and the company in question has to repair the damage (Solutions, 2014).

2.3.2. Information Security Risk Analysis

Peltier (2005) maintains that it is almost impossible to determine the level of security an organisation needs to keep its systems safe from intrusions and that, in some cases, an information security risk analysis raises more questions than it answers. Nevertheless, an information security risk method may be of tremendous benefit to an organisation and may play a very important role in an organisation's success. An information security risk analysis may help an organisation to measure its economic loss resulting from problems occurring in its information security processes (Feng, Wang & Li, 2014) and provides an organisation with increased knowledge and a greater depth of understanding of its expected loss due to security failure (Ryan & Ryan, 2006). However, it is vital that an organisation ensures that the information security risk methodology employed corresponds with international best practice and is appropriately adapted to the organisation's particular environment (Albert & Dorofee, 2003; Alnatheer, 2009; ISACA, 2009).

2.3.3. Risk Assessment

Risk assessment is useful in determining the extent of the potential threat and risk to which an employee may be exposing the organisation (Williams, 2008). The output of this risk assessment process helps in the identification of appropriate controls for either reducing or eliminating the risk. The insider threat may not be malicious and may be uninformed, the result of cultural beliefs, mistakes and/or errors, or be attributed to a lack of policy and procedures. Addressing these issues requires that both technology and the people are taken into account as well as an encompassing security governance approach. The security governance approach is a method of pursuing strategic goals by balancing risk with return on investment. It includes accountability, it allows for the demonstration of appropriate practice and integrity and it means that everyone in the organisation is involved (Williams, 2008).

It is important to identify what must be protected and its value to the organisation. ***Risk = Value x Threat x Vulnerability*** is an accepted risk assessment equation (Stoneburner, Goguen & Feringa, 2002). The greater the value of the information to

the organisation, the greater the risk of damage to the organisation if any threat and vulnerability exist. However, often the perception of threat is overestimated in relation to the value of the information and, therefore, a perceived risk is accorded more credence and attention than is, in fact, required to protect that information (Williams, 2008). In addition, the impact of any effective threat, particularly in terms of workflow and ability to continue with the organisation's primary function, should also be taken into account. Thus, a defined process for risk assessment is required while a balanced response to treats must be predefined.

2.3.4. Threats and Vulnerability Identification

Vulnerability is a measure of the exploitability of the weakness that encompasses the business processes, communication systems, and information technology supporting the mission of the organisation (Sarkar, 2010). With both the increased capability and reliability of personal computers and the availability of end-user packages, responsibility has therefore shifted to the employee. However, the employees who now possess all these responsibilities are generally not trained in the information technology field and, therefore, they do not possess the skills required to behave in a secure manner, thus resulting in vulnerability (Hasan, Zawoad, Noor, Haque & Burke, 2016). For example, using passwords to control access to data would be useless if the computer housing the data could be carried out of the door because a user has left the door unlocked, or if the user posted the password next to the screen. In other words, operational controls are now required to dictate to and ensure that users operate in a manner that does not undermine the physical and technical controls which are in place (Layton, 2016).

Engineering SMEs often assume a minimum vulnerability of their parts and are of the perception that security is not an issue for them as there is significant employee trust (PricewaterhouseCoopers, 2014; Williams, 2009). However, ironically security is more important for SMEs than larger organisations, as SME employees often fulfil multiple roles and thus they have access to a variety of financial, organisational, customer and employee information, as well as access to multiple services such as

the internet and email. Furthermore there is less segregation of duties in SMEs and thus less control over access to information compared to larger organisations (Williams, 2009). While SMEs are exposed to the same threats and vulnerabilities as large organisations, they do not, however, have access to the same level of resources in order to secure their information.

The low vulnerability perception of SMEs may be attributed to the fact that almost three-quarters (72%) of insider incidents are not publicly known as these incidents are usually handled internally without legal action or the involvement of law enforcement (PricewaterhouseCoopers, 2014). Nevertheless, the cybercrimes committed by insiders are often more costly and damaging than attacks from outside (CSO Magazine, 2010; PricewaterhouseCoopers, 2014).

Williams (2008) defines threat as human error, intellectual property compromises, unauthorised access, information extortion, sabotage, theft of information, disruption in availability of information and software attacks. On the other hand, Sarkar (2010) identifies threats in a slightly different way as the inappropriate use of devices, network data breaches, laptop loss/theft and lack of education. However, this study viewed threat as a combination of both these definitions.

The uninformed employee may cause risk to the organisation's information asset by responding to phishing emails, visiting malicious software (malware) infested websites, sharing or using weak passwords, storing their login information in unsecured locations, or giving out sensitive information by failing to detect social engineering.

2.3.4.1. Malware

Malware refers to contaminant software which is designed to secretly access a computer system without the owner's informed consent (Oxford English Dictionary, 2002). Software is considered to be malware based on the perceived intent of the creator rather than on any particular features. Malware includes computer viruses,

worms, Trojan horses, spyware, dishonest adware, scareware, crimeware, most rootkits and other malicious and unwanted software programs. Chau, Nachenberg, Wilhelm, Wright & Faloutsos (2011) suggested that the release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications. According to F-Secure, the malware produced in 2015 alone exceeded the total malware produced in the previous 20 years. Malware's most common pathway from criminals to users is through the Internet, primarily by e-mail and the World Wide Web.

2.3.4.2. Phishing

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication (Allam et al., 2014). Communications purporting to originate from popular social websites, auction sites, online payment processors or IT administrators are commonly used to dupe the unsuspecting public. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter their details on a fake website whose look and feel are almost identical to the legitimate website. Phishing is an example of the social engineering techniques used to mislead users and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

2.3.4.3. Passwords

Computer users should choose their passwords carefully. The aim is to choose a password that will minimise the chance that somebody will be able to work it out. According to Boeckeler (2004), a strong password is one that

- does not contain any words found in a dictionary
- does not contain any words that are of significance to the user
- does not contain any numbers that are of significance to the user, e.g. birthday
- is not a variation of 1, 2 or 3.

For example “cowboy” is an example of a weak password. However, changing it to “CowB45oy” makes it a much stronger password.

Lastly, it is never advisable for employees to keep their passwords on a post-it note underneath their keyboards or on their screens. It is pointless for the employees to even bother having passwords in the first place if these passwords are going to be accessible to anyone who wants them.

2.3.4.4. Social Engineering

Social engineering is the act of exploiting human weaknesses and manipulating people into performing actions or divulging confidential information instead of breaking in or using technical cracking techniques (Weaver, Furr & Norton, 2016). The organisational cultures of SMEs are often characterised by a high level of employee trust. However, this trust is not conducive to effective security, particularly in instances in which certain attack strategies such as social engineering exploit such trust (Weaver, Furr & Norton, 2016). An example of this may be telephoning a secretary at an organisation, pretending to be the organisation’s IT technician, making up a lie such as there is regular maintenance scheduled on her computer after hours, encouraging them to divulge their password which they then unsuspectingly do (Newbould & Furnell, 2009). As a result of the trust in the organisational culture the victim employee does not bother to verify the request. Social engineering is a legitimate strategy used by serious hackers with some of the most infamous and successful hackers having become very skilled at it (Boeckeler, 2004).

When exploiting the greed of the potential victim, the attacker suggests to the victim that they will receive a large amount of money in return for sending a small amount of money first, usually explained as a release fee, bribe or legal fee. Other forms of such an attack may involve the attacker posing as a victim of a recent natural disaster and trying to exploit the victim’s sympathy. Although the majority of the

recipients of such emails do not respond, there will always be a small, but tangible, proportion that does.

2.3.5. The Consequences of the Risk

Data loss, whether from internal or external sources, remains an overwhelming concern. The number of organisations investing in data loss prevention (DLP) solutions leapt to 44% in 2009 as compared to 29% in 2008. It has been found that only six out of ten organisations possess an accurate inventory of the location of all their data and where and when it is collected and transmitted. Clearly, further commitment and investment in technology and education are required (SCMagazine, 2010).

2.3.5.1. Consequences to the Employee

- Dismissal from work
- Suspension from work
- No/low bonuses
- Spam, which is defined as “the abuse of any electronic communications medium to send unsolicited messages in bulk” to as many users as possible (Elliot, 2011).
- Theft of personal information

2.3.5.2. Consequences to the Organisation

It emerged from the findings conducted of the survey conducted by PWC in its Global State of Information Security Survey (2015) that approximately 75% of the organisations which were victims of employee security breaches did not report for legal action. According to a 2010 survey (CERT, 2010), the reasons for not reporting include the following: the damage level was not significant enough to warrant prosecution, lack of evidence, the individuals could not identified and fear of negative publicity. As a result, organisations risk hiring employees who behaved in an insecure way in their previous jobs. The consequences of attacks on the organisation include, but are not limited to, the following:

- **Data corruption** – An intentional modification, insertion, deletion of operating system or application system programs, whether by an authorised user or not, which compromises the confidentiality, availability or integrity of data, programs, system, or resources controlled by the system. This includes malicious code such as logic bombs, Trojan horses, trapdoors and viruses (Elky, 2004).
- **Bandwidth abuse** – The accidental or intentional use of communications bandwidth for other than the intended purposes (Elky, 2004).
- **Denial of service –** Denial of service (DoS) refers to an intentional or unintentional assault on the availability of a system (Elliot, 2011).
- **Leaking/theft of corporate data** – The unauthorised or accidental release of classified, personal, or sensitive information (Elky, 2004; Sarkar, 2010).
- **Reputational damage –** Most companies try to avoid public announcements on insider abuse as such publicity may have a negative effect on brand integrity and the reputation of the entire industry. Any insider attack, when made public, has a direct impact, such as a loss of customer confidence, loss of customers to competitors and a huge financial loss as a result of restoring normal service or sorting out resultant issues (Sarkar, 2010).
- **Ransomware –** Criminals possess the capability to encrypt a victim's hard drive leaving just a Readme.txt file which instructs the victim how to contact them in order to purchase the decryption key (Elliot, 2010).
- **Service disruptions –** Service disruptions may have a significant impact on businesses mainly because it usually takes time before service is restored, thus hampering the organisation's ability to complete transactions timeously.
- **Financial Losses –** Loss of organisational faith on the part of clients as well as reduced business as service disruptions may lead to reduced business and these may in turn result in losses.
- **Exposure –** Confidential client databases or organisations trade secrets may be leaked, thus affecting brand integrity as well as the organisation's competitive advantage.

2.3.6. Risk Mitigation

There are certain risk mitigation strategies that organisations may use to minimise the risks from common security threats. The most effective of these strategies include user awareness campaigns, implementing security controls, firewalls, intrusion detection systems, intrusion prevention systems, anti-virus software and insurance as well as enforcing strong policies. These strategies fall into one of the following defence categories, namely, transference, acceptance or avoidance. This study focused on avoidance, although all three are briefly explained below:

2.3.6.1. Transference/Sharing

Risk sharing may be defined as sharing with another party the burden of loss or the benefit of gain arising from a risk and the measures taken to reduce a risk (Elky, 2004). Risk sharing usually involves purchasing an insurance contract in order to transfer the risk. However, technically speaking, the organisation generally retains legal responsibility for the losses "transferred", thus meaning that insurance may be described more accurately as a post-event, compensatory mechanism. For example, a data loss insurance policy does not transfer the risk of data loss to the insurance company and the risk still lies with the policy holder, namely, the organisation. The insurance policy merely ensures that, if there is data loss (the event), then some compensation may be payable to the policy holder that is commensurate with the suffering/damage. In practice, if the insurance company goes bankrupt or the claim goes to court, the original risk may revert to the organisation.

2.3.6.2. Acceptance

Acceptance involves accepting the loss, or benefit of gain, arising from a risk when it occurs. Risk acceptance is a viable strategy in the case of small risks where the cost of insuring against the risk would be greater over time than the total losses which may be sustained (Elky, 2004). All risks that are not either avoided or transferred are retained by default. This includes risks that are so large or catastrophic that it is either not possible to insure against them or the premiums would be infeasible. War is such an example since most property and risks are not insured against war, and, thus, loss

arising as a result of war is retained by the insured. In addition, any amounts of potential loss (risk) over the amount insured constitute retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great that it would compromise the goals of the organisation.

2.3.6.3. Avoidance

Risk avoidance involves not performing an activity that could carry risk (Elky, 2004). An example of risk avoidance would be not networking computers and not connecting them to the internet as this would expose the inside information to the outside world. Although avoidance may appear to be the solution to all risks, avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed, For example, not entering into a business deal to avoid the risk of loss also avoids the possibility of earning profits from the deal.

There is no total solution for risk avoidance of information security risks and threats. Nevertheless, antivirus software, firewalls and awareness campaigns are some of the commonly used risk avoidance control measures. These are explained next.

1. Antivirus Programs

Antivirus programs typically work in two different ways. Firstly, they contain a database of signatures of all known viruses and worms. The software searches a computer for the presence of these signatures. In view of the fact that new viruses and worms are found almost every day, these databases are regularly updated by the antivirus software developers. The second way in which antivirus software operates is by looking for suspicious activity such as when a virus actually tries to infect a file (Boeckeler, 2004). For example, some viruses change the size of a file when they infect the file. However, this may be easily detected by an antivirus program. On the other hand, virus writers know that antivirus programs look for changes in file size and thus they have devised ways to infect a file without increasing the file's overall size.

2. Firewalls

A firewall is a device that sits between a computer or network and the outside internet. It is designed to be the main defensive barrier against intruders. Traditionally, firewalls were a hardware device, but today there are both hardware and software firewalls (Boeckeler, 2004).

Hardware firewalls are basically a chokepoint. All network traffic must pass through the firewall before it may enter the network. Most firewalls operate in accordance with a set of rules. These rules must be set up by the administrators of the network and they instruct the firewall what to do under various conditions. There are different types of hardware firewalls, varying in sophistication. Organisations that use hardware firewalls often also use an application called an Intrusion Detection System (IDS). Intrusion Detection Systems often run on a separate computer that receives everything that passes through the firewall. They are designed to identify suspicious activity and alert the network administrators when necessary. In addition, firewalls may help organisations to learn from an incident and better prepare for the future (Boeckeler, 2004).

Software firewalls, such as ZoneAlarm and BlackIce, run on Windows based personal computers and include considerable IDS functionality. Once installed, these programs monitor both what is coming into the computer as well as what is leaving it. Thus, they are able to detect all sorts of external activities directed towards the computer from port scans to a flood attack. Also, since they monitor traffic from a PC to the outside network, they are able to alert the employee to the presence of unknown malicious software, such as a virus or worm that is using the computer to conduct a DoS attack. These firewalls keep a close track of the programs which are allowed to access the Internet and which are not. The configuration is usually straightforward. In addition to monitoring, all traffic that goes in and out of a system, firewalls are also able to effectively hide the computers on which they are installed from the outside internet. It is not possible for hackers to break into a computer if they

do not know it exists. As a result, when someone does try to conduct a port scan on a computer (really the IP address) running a firewall, the person will learn nothing from it (Boeckeler, 2004).

3. Information Security Awareness

The previous sections highlighted how a non-malicious employee may be a risk to the organisation. However, awareness campaigns and training may help minimise this risk. The existence of a formal security policy does not necessarily mean that the employees are aware of it/understand the policy and, therefore, will adhere to it (Herath & Rao, 2009). It is, thus, essential that they are made aware of the security practices prescribed in the policy. An information security awareness and training program is best suited for educating employees. Information security awareness is a component of an organisation's information security program and is an initiative that aims to change employee attitudes and behaviours by educating them about safe security practices (Yildirim, 2016). This ensures that employees realise the importance of security as well as the adverse consequences of security failure. Security awareness means understanding that there is potential for some people to deliberately or accidentally steal, damage or misuse the data which is stored on an organisation's computer systems and elsewhere in the organisation (Kabay, 2005).

Security awareness programmes are typically divided into two different, yet related, components, namely, awareness and training. The goal of awareness is to raise the collective awareness of the importance of security and security controls while the goal of training is to facilitate a more in-depth level of user understanding than may otherwise have been the case (Krutz & Russell, 2001). An effective information security awareness and training programme explains the proper rules of behaviour governing the use of the organisation's information and communication technology (ICT) systems and information assets. Thus, the programme communicates the ICT security policies and procedures that must be complied with. However, in order to increase the chance of compliance, this must be followed by communicating the

sanctions that may be imposed in the event of noncompliance. Users must also be informed initially of expectations while accountability must be derived from a fully informed, well-trained and aware workforce (Hunter, 2000; Wilson & Hash, 2003).

According to Von Solms and Von Solms (2004), not implementing an information security awareness program is one the ten deadly sins of information security management. It is vital that SMEs realise that employees, whether intentionally or unintentionally, pose the greatest threat to information security, often as a result of a lack of knowledge (Brodie, 2008). Although information security awareness is only a single component of a broader information security programme, its lack or weakness has implications for the realisation of overall information security goals (Eminağaoğlu et al., 2010; Pfleeger & Caputo, 2012; Wilson & Hash, 2003). It is a known fact that it is not possible to totally eliminate the information security risk to an organisation (Flowerday & Von Solms, 2005). In fact, eliminating the risk would entail ceasing operations. However, a well-planned employee security awareness programme may help to reduce the risk to acceptable levels. Awareness campaigns are critical because they help employees to understand their role in reducing the risk and protecting information assets (Chipperfield & Furnell, 2010; Krutz & Russell, 2001; Russell, 2002).

2.4. Current Insider Statistics

Unfortunately, there appear to limited statistics on computer crime in South Africa. However, generally speaking, computer systems all over the world are prone to the same threats and, thus, an assumption is made that the Australian, British and American statistics are similar to those in South Africa.

The debate around the origin of threats is supported by a global, online, E-Crime survey which was conducted by CERT in 2011. The respondents were asked who caused costly damages, either insiders or outsiders. The results were clos, namely, insiders 33%, outsiders 38% and unknown 29%. The findings also indicated that the participants were not according the importance to insider threats that would seem

justified. Confidentiality, integrity and availability all represent aspects of the information assets being protected (ISO 27002, 2013). According to the Schulze's (2016) report, 56% of the respondents felt that insider threat was on the rise while 44% were unsure. However, 74% of these respondents indicated that they felt vulnerable to insider threats. People, process and technology all play equally important roles in information security. However, technical controls, such as firewalls, often receive all of the attention and people and process are overlooked. It is often just awareness that is the key to prevention of attacks and the protection of valuable organisation information assets. Nevertheless, it would appear that SMEs invest the most in technological (physical) protection e. g. antivirus and firewalls although, in reality, the employees control the technology. It is, thus, important to educate the employees in that respect (Pfleeger & Caputo, 2012; Russell, 2002; Stephanou & Dagada, 2006). An organisation may be bristling with firewalls and antivirus systems, but a naïve user may allow an attacker in through the back door (Chipperfield & Furnell, 2010; Power, 2002).

CERT's 2007 E-Crime Watch Survey (2007) found that insiders (34%) were fairly close to outsiders (37%) in causing the most damage, However, nine years later, insider risk had gone up to 56% (Schulze, 2016). The CERT's 2010 E-crime Survey (2010) indicated that, while outsiders were the main culprits in cyber-crime, it was insiders who were the cause of the most costly and damaging attacks.

Key findings from the 2009 CSI computer crime and security survey shows 43.2 % of respondents stated that at least some of their losses were attributable to malicious insiders. But, clearly, non-malicious insiders are the greater problem. 25% of respondents felt that over 60% of their financial losses were due to non-malicious actions by insiders; however, their 2010 information security breaches survey shows a 26% increase in the insider threat comparing to the previous year.

According to Schulze's (2016) report, inadvertent data breaches (e.g. careless user causing accidental breach) top the list of the insider threats to which organisations pay the most attention, namely, 71%. Negligent data breaches (e.g. user wilfully ignoring policy, but not maliciously) were second at 68% and malicious data breaches (e.g. user wilfully causing harm) third at 61%. This survey also reported that privileged IT users, such as administrators with access to sensitive information, posed the biggest insider threat (60%) followed by contractors and consultants (57%) and then regular employees (51%).

A 2005 survey commissioned by McAfee was revealing in terms of both employee behaviour and awareness. Among the undesirable practices the findings suggested that 21% of workers allowed family and friends to use their employers' computers to access the internet, while 10% admitted to downloading inappropriate content at work. In terms of awareness, 62% admitted a limited knowledge of IT security, with 51% not even knowing how to update the anti-virus protection on their work PCs. The awareness problem appeared to have been a less serious by 2016 as most organisations (72%) are now offering training to their employees on how to identify security risks (Insider Threat Spotlight Report, 2016).

Sarkar (2010) provided statistics on the types of insider misuse and how organisations view insider threats: It was found that, in the main, insider activities revolve around stealing, destroying or modifying data. These activities may be classified as misuse under information systems, external websites and internal networks:

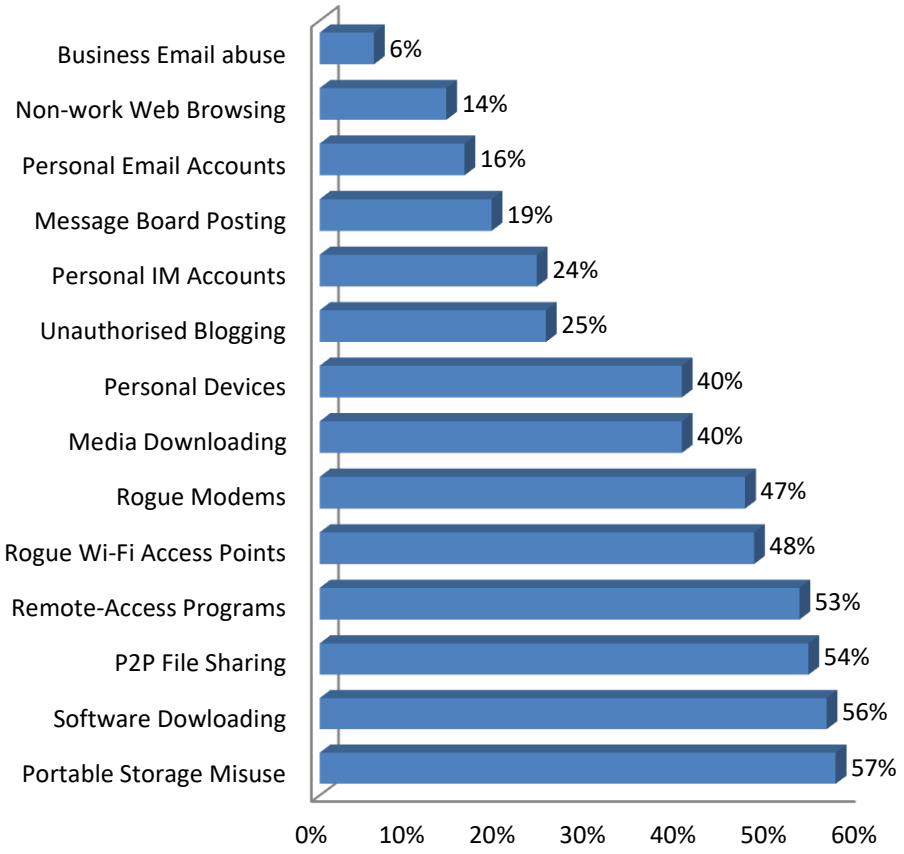


Figure 2.5: Percentage of Organisations Viewing Type of Insider Misuse as Major Threat (Sakar, 2010)

The surveys all clearly indicate that insider threats are becoming more of an issue and also more wide spread than accounted for. One reason is the use of non-technical means, such as social engineering by insiders, to gain unauthorised access to and compromise an organisation's sensitive data. In view of the fact that organisations are fortifying their perimeters, criminals are using more sinister means to gain access to an organisation's proprietary information by 'planting' insider threats (Sarkar, 2010). This insider 'time bomb' is compounded by several factors, including the following:

- Many organisations do not report insider misuse and, thus, it is difficult to estimate the scale of the problem.
- Employees are merging their working lives with their private lives.
- Organisations are introducing a mobile work force and, thus,the perimeter is becoming more porous. Employees are carrying sensitive data on laptops,

mobiles and USBs which, when lost or stolen, compromise the data (Sarkar, 2010).

2.5. Conclusion

An understanding of the human element in an information security management framework as well as individuals' perceptions of information security and their motives behind compliance should impact on the type of preventative actions taken and also reduce the number and severity of security related incidents. One of the best ways in which to make sure that employees do not make costly, unintentional errors in respect of information security is to institute a company-wide, information security-awareness programme. This will help the attempt to achieve a sound understanding of the organisation's security policy, procedure and best practices by employees (Brodie, 2008; Montesdioca & Maçada, 2015; Puhakainen & Siponen, 2010).

Many in the information security profession agree that, in order to realise an improvement in information security, it is essential that the human factor issue is addressed. This may be done by training, educating and increasing awareness but, ultimately, this is sustainable only if a security culture is promoted and adopted. The weakest link in the security chain remains the human factor. Therefore, not only should sound security procedures be put in place but practices that support sustainable change and the adoption of best practice should be instituted. In essence, what is needed is the creation of an intuitive security culture. The information security profession is, thus, charged with facilitating this change although, arguably, this is a more difficult challenge than merely implementing sophisticated technical solutions.

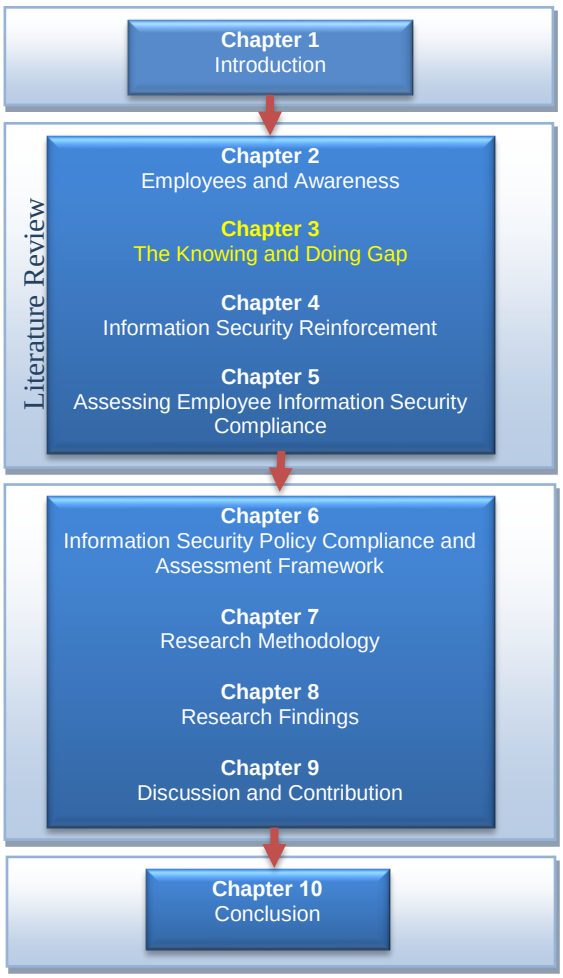
The more lines of defence an organisation has in place, the less likely there will be a successful breach. Although, multiple layers of technology such as firewalls, network intrusion detection systems, bastion hosts, etc. increases lines of defence, results of surveys and analyses, clearly indicate the most serious threat to the information environment is often from the employee. Hence, the employees should be made the

organisation's first line of defence by equipping them with the required knowledge through information security awareness campaigns.

Technical solutions may only protect information up to a point and, thus, the human aspect of security has become a major focus of discussion. It is therefore important for an organisation to create a security awareness platform that focuses on employee behaviour, because an organisation's success or failure effectively depends on what its employees either do or fail to do in respect of information security.

If employees are not engaged in the protection of information then breaches will occur. Education, reinforcement and integration with day-to-day activities are essential to the success of any information security initiative. Creating an environment in which every employee sees him/herself as a valuable part of the security initiative will ensure the sustainability of the initiative and enhance the protection of important information. The next chapter discuss the methods used for ensuring a trusted information security aware environment.

CHAPTER 3 - THE KNOWING AND DOING GAP



Chapter 3:

This chapter discusses the information security knowing and doing gap (omissive behaviour). Various information security awareness techniques are identified and discussed in order to obtain an understanding of the reason why the gap exists. The chapter also attempts to identify the relationship between information security awareness campaigns, knowledge gained through them and the actual behaviours resulting from campaigns.

3.1. Introduction

Information security awareness and training initiatives are intended to increase existing knowledge about security. Information security awareness refers to a state in which the users in an organisation are aware of and, ideally, committed to the organisation's security mission (Dlamini, Eloff, & Eloff, 2009); Nosworthy, 2000; Pfleeger & Caputo, 2012). According to Öğütçü et al. (2016) and Drevin, Kruger and Steyn (2007), increasing the awareness of security issues is the most cost-effective control that an organisation may implement. Ifinedo (2014) suggests that the absence of awareness programmes indicates a critical gap in effective security implementation. Security training and awareness programmes are, therefore, a fundamental component of an effective information security strategy as they may help organisations to minimise the potential damage caused by uninformed or misinformed employees (Allam et al., 2014; Drevin et al, 2007; Eminağaoğlu et al., 2009).

In the main, an organisation's management communicates formal company direction, rules and regulations through the organisation's policies. These policies are usually either written (hard copies) or communicated verbally during employee induction. A copy may also be available on the organisation's intranet/SharePoint site. Information security policies provide a solid foundation for the development and implementation of secure practices within an organisation. These policies present the rules that must be adhered to. Compliance with the rules, however, requires an understanding of not only the individual policies but also of the circumstances in which such compliance is expected during the employees' day-to-day activities (Bacik, 2008; Ashenden, 2015; Kajzer, D'Arcy, Crowell, Striegel & Van Bruggen, 2014; Johnson, 2006; Talbot & Woodward, 2009; Von Solms, 2001).

In general, security awareness efforts are designed to change behaviour or to reinforce good security practices (Eminağaoğlu et al., 2010; Wilson & Hash, 2003). Effective information security awareness programmes may, ultimately, improve the

organisation's efficiency as these programmes will allow the organisation to focus on techniques that improve the employees' intentions and, ultimately, encourage employees' security behaviour in the interests of a more efficient enterprise (Stephanou & Dagada, 2006).

At the time of the study the effectiveness of security compliance drives was still uncertain as, regardless of their knowledge, some employees do not fully comply with their organisation's security policies (knowing and doing gap) (Shropshire et al., 2015; Siponen, Mahmood, & Pahnila, 2014). This may be attributed to the myth that the assessment of behavioural intentions is a close reflection of actual behaviours. However, there is an undeniable gap between knowing and doing (Goo et al., 2014).

This chapter discusses the reason why information security is an issue. It then goes on to discuss how security awareness assists in increasing knowledge which encourages compliance. The chapter then addresses the problems associated with the conversion of intention to behaviour and, finally, the chapter discusses focuses on testing for a relationship between intention and behaviour.

3.2. Is Information Security Awareness: Really an Issue?

The findings of a survey conducted by the multinational advisor group KPMG (1998) in conjunction with the research group BMI-TechKnowledge (in Du Plesis & Von Solms, 2002) showed that 66% of all the respondents possessed limited information security knowledge and viewed information security as unimportant to the organisation. Ten years later Schneier (2008) found that 62% of employees still had limited information security knowledge, while 18 years later PWC (2014) revealed that 51% still had limited information security knowledge. This shows an average increase of 1% per year. At this rate it would take 50 years to achieve reasonable security awareness levels. This highights the urgent need to come up with solutions as this awareness issue helps to exacerbate the lack of information security compliance. Richardson (2008) also revealed that 18% of respondents had not undergone any awareness training at all while, of those who had had awareness

training, 32% had done nothing to measure the effectiveness of the approaches they used. In view of the concept of information warfare, it is imperative that security awareness is part of an organisation's first line of defence.

Employees with 'little-to-no' prior security training or experience may suddenly become responsible for thousands of records with sensitive data as part of their jobs. An understanding of information security as a result of a well-structured information security awareness programme is, therefore, crucial to significantly minimising the security risk. Often the weakest link in information security is not the technology but the employees who control the technology. The weakness which employees represent may never be totally eliminated but a well-structured security awareness campaign helps to reduce the risk to acceptable levels (Johnson, 2006; Krutz & Rusell, 2001). However, Wright et al. (2009) suggest that an individual's perceptions of security may vary over time and in different situations. This further complicates threat and vulnerability assessment initiatives. As a result, it is essential that any awareness program are continually measured and managed to ensure an up to date knowledge of any changes in risk profiles (Kruger & Kearney, 2006). In order to ensure that the users' knowledge remains current and their memories are refreshed, an awareness program must be both ongoing and be an integral aspect of an organisation's information security culture.

The development of information security policies and campaigns is a lengthy process that requires time, money and specialised knowledge. These constraints may prove prohibitive for small to medium-sized companies and may be a possible cause for the low level of security awareness in these organisations (Du Plessis & Von Solms, 2002). The small number of organisations implementing awareness programmes and the low level of awareness within organisations suggest that these approaches are also ineffective (Du Plessis & Von Solms, 2002).

3.3. How does Information Security Awareness Assist?

Awareness campaigns are intended to alter employee behaviour (Allam et al., 2014). In turn employee behaviour plays an important role in the information security stance of organisations. The majority of SMEs develop and communicate information security policies (i.e. information security rules and regulations) which are aimed at governing and supporting employees. These policies normally define the tolerable use of computer resources, employees' responsibilities regarding information security and the consequences of security policy noncompliance. These policies are drafted with the belief that the behaviour mandated in them will achieve the desirable compliance. However, the literature suggests that more than half of all of information security breaches are caused by employee noncompliance with the organisational information security policy (Bulgurcu et al., 2010; Alotaibi, Furnell, & Clarke, 2016).

3.4. Awareness and Training Supporting Frameworks

The first step in developing an effective information security awareness programme is to ensure that a security policy has been formulated. The policy should comply with the ISO/IEC 27001:2013, ISO 9001:2015, POPI or the COBIT. In addition, the policy should be drafted in a clear and concise manner, and accurately reflect the organisation's overall stance on security.

An effective information security awareness and training programme seeks to explain the proper rules of behaviour when using the organisation's computer systems and information. Thus, the programme communicates the information security policies and procedures that need to be followed. Such a programme must precede and impose sanctions in the event of noncompliance. Employees must also be informed of expectations such that accountability is derived from a fully informed, well-trained and aware employees (Herath & Rao, 2009).

3.5. Organisational Roles and Responsibilities in respect of Information Security Awareness

Experienced security personnel or willing non-security personnel within an organisation may be put to great use by appointing them to write articles, attend topical meetings and make presentations (Van Loenen, 2015). This association may also be beneficial as respected organisational employees may add weight to the security awareness programme. Another important aspect of using in-house personnel for awareness training is that, over time, trusting relationships may be built up among the experienced personnel.

There are many reasons to outsource security awareness training. However, the most common reason is that is usually relatively easy and quick to utilise the skills of a professional security awareness training company, especially if speed is of the essence (Van Loenen, 2015). Some companies specialise in particular aspects, such as awareness videos, newsletter creation, posters, or item customisation (mouse pads, pens, etc.). There are also some free sources of security awareness materials which offer features such as screen savers, security best practices or other educational materials. An organisation may outsource almost any security awareness material if it either cannot or does not wish to use free online sources or use security awareness vendors. Each programme director must, of course, decide what is best for the organisation's information security programme.

3.6. Awareness, Training and Education

Security training and awareness should begin during new-hire orientation to establish the organisation's commitment to security at an early stage of employment. Educating an employee six months after he/she has started work may be too late as bad security habits may already have been formed. Awareness activities should be almost perpetual, yet interesting enough so that they are not ignored.

Kruger and Kearney (2005) highlight the absence of a simple solution to creating an effective and secure information environment. However, SMEs should keep in mind that one of the key aspects to improved security is to raise the general level of information security awareness and also to educate all employees on the basic elements of information security. Researchers such as Van Loenen (2015) and Allam, Flowerday and Flowerday (2014) suggest the importance of awareness practices that may influence employee security-related behaviour. Such efforts have resulted in a stream of information security research, focusing on behavioural elements together with organisational and managerial initiatives (Goo et al., 2014; Hearth & Rao, 2009; Puhakainen & Siponen, 2010; Stanton et al., 1999).

There are many reasons why organisations implement information security awareness programmes, however the following are the most universal according to the literature, namely to ensure that:

- Employees (users) are informed about the existence and contents of the organisation's information security policy and that they must adhere to it (Johnstone, 2001; Peltier, 2005; Pfleeger & Caputo, 2012; Allam et al., 2014).
- Employees are aware of their role in helping to protect the confidentiality, availability and integrity of the organisation's information assets (Hunter, 2000; Johnstone, 2001; Stephanou & Dagada, 2006; Talaei-Khoei et al., 2012; Durcikova, & Jennex, 2017).
- Employees understand why, how and from what/whom they are protecting the information assets (Danchev, 2003; Eminağaoğlu et al., 2010; Van Niekerk & Von Solms, 2004).

Organisational security awareness influences employee behaviour and attitudes while upper management sets the tone for information security through policies, ethical expectations and an emphasis on proper procedures. The employees' attitudes towards adhering to the established policies and procedures are influenced by knowledge, personal ethics and acceptable behaviour (Williams, 2008). However,

individual attitudes may affect intended behaviour but not always actual behaviour as employees often want to behave one way but actually behave in another way, e.g. the privacy paradox.

Lee, Yoon, and Kim (2008) are of the opinion that employees tend to behave in a manner that is consistent with their perceptions of the group's normal behaviour. According to the TPB this refers to the subjective norms construct. Security awareness and training assist in tempering employees' attitude that security policies are restrictive and interfere with their ability to perform their work while also fostering improved incidence reporting. The better the employees' understanding of security issues, the more they understand both the importance of security as well as the ways in which security protects and enables them to do their jobs in a more effective environment (Johnston, 2001; Pfleeger & Caputo, 2012).

Information security awareness campaigns comprise two different components, namely, awareness and training. Awareness aims at raising the collective awareness of information security and its controls while the training aims at facilitating a more in-depth level of employee information security understanding. An effective information security awareness and training programme seeks to elucidate the proper rules of behaviour when using the organisation's ICT systems (Herath & Rao, 2009; Safa et al., 2015; Talaei-Khoei et al., 2012).

However, awareness programmes alone are not enough. While they may serve to focus attention on security issues, they still do not ensure that staff members are personally equipped to deal with these issues. However, it is information security training that then establishes and fosters the necessary knowledge and skills to enable employees to successfully protect information assets (Colwill, 2009; Furnell & Thompson, 2009).

Nevertheless, training should not involve a ‘do not do this’ programme. The learning objectives of the programme should be the inculcation of the skills required to support the corporate information security policy. Training should certainly promote the policy and procedures but it should also be designed to instil a concept of best practice and understanding among the employees (Öğütçü, 2016). The organisation may consider the programme to be successful if all the employees who have completed the training are entirely convinced and motivated by one fundamental belief: namely, that information security is part of their responsibilities and that they possess the skills required to fulfil these responsibilities.

3.7. Developing Awareness and Training Material

The first step in developing awareness initiatives is to create a mental image of the objectives to be accomplished. This mental image will then be transformed into words and actions to be presented to the employees. Effective communication methods should, thus, be used. According to Bacik (2008), a two-way process between the sender of information and the receiver of the information is the most effective method of communication as compared to a one way method of communication. Communication with employees usually takes the form of talking, reading, watching, listening and observing activity. According to Kruger and Kearny (2006), information security awareness campaigns communicate the specific operational steps that employees must take to achieve the goals of the organisation’s policy.

3.7.1. Selecting Topics for Training

The main discussion of the awareness campaigns should be centred on the organisation’s security policy. This policy establishes the security direction for the organisation, and knowledge of this policy will help the employees to understand what the organisation is striving for in information security (Safa, et al., 2016). It would be impossible to cater for such organisation specific information in a generic programme. In order to understand why they need to protect information, employees also need to be aware of the threats to, and vulnerabilities of, computer systems (Chipperfield & Furnell, 2010). The material used in awareness campaigns would

include security important topics such as viruses, password construction, password management, laptop security while travelling, physical security, hacking, denial of service (DOS), spoofing/sniffing data confidentiality, wireless security, home office security, privacy, identity theft, internet use, email use, data backups, Intellectual property rights, encryption and the concept of social engineering (Johnson, 2006).

3.7.2. Finding Sources of Awareness and Training Material

There are a variety of sources of material on security awareness that may be incorporated into an awareness campaign. The material may address a specific issue or, in some cases, it may describe how to begin to develop an entire awareness campaign or session. Sources of such material may include:

- E-mail advisories issued by industry-hosted news groups, academic institutions, or the organisation's IT security office;
- Professional information security organisations and vendors;
- Online IT security daily news websites;
- Periodicals; and
- Conferences, seminars and courses.

3.8. Techniques for Communicating Awareness Material

This section discusses the techniques for communicating information security. Communication within an organisation occurs in many different ways but is usually described in terms of either horizontal or vertical mechanisms. Horizontal (or sideways) communication is more informal as compared to vertical communication and takes place between colleagues working on the same level (Chipperfield & Furnell, 2010). Many organisations rely heavily on vertical (downwards) communication which is information passed from the top down through line managers and in official communications.

Awareness material may be developed using one theme at a time or by combining a number of themes or messages into a presentation. For example, a poster or a slogan on an awareness tool usually contains one theme, while an instructor-led

session or web-based presentation may incorporate numerous themes (Wilson & Hash, 2003). However, regardless of the approach taken, the amount of information presented should not overwhelm the audience. The major topics to be included in a typical awareness presentation include a brief mention of requirements (policies), the problems that the requirements were designed to remedy, and the actions to take are.

3.8.1. Channels of Communication

The BERR (2008) survey provided some relevant findings which suggested that the majority of organisations tend to rely upon written materials in some form. However, merely developing and circulating a policy or directing employees to an intranet page that details security procedures are not sufficient to foster appropriate security understanding and behaviour. An information security awareness programme is essential and aim of such a programme should be to focus the employees' attention on information security and move them from the 'naïvety' level to the 'awareness' level (Chipperfield & Furnell, 2010).

By introducing similar security awareness material in a variety of ways the employee is exposed to the topic more than once and, thus, will retain information better (Kajzer, D'Arcy, Crowell, Striegel and Van Bruggen, 2014). Before any communication is disseminated, it is vital that the presenter understands whom the audience will be and why the audience is being exposed to the communication. Although the topic may not change, the way in which it is communicated may change depending on the audience (Bacik, 2008). The communication may utilise both formal and informal methods of instruction. Formal instruction methods include security awareness tutorials, training courses, testing, formal presentations of security policies and/or professional articles in newsletters. On the other hand, informal methods may include brief newsletter articles, quick notes, lunch meetings, discussion groups, screen savers, posters and physical reminders such as mouse pads, pens or tension squeeze balls. Figure 3.1 depicts some of the ways in which an organisation's information security policy may be communicated.

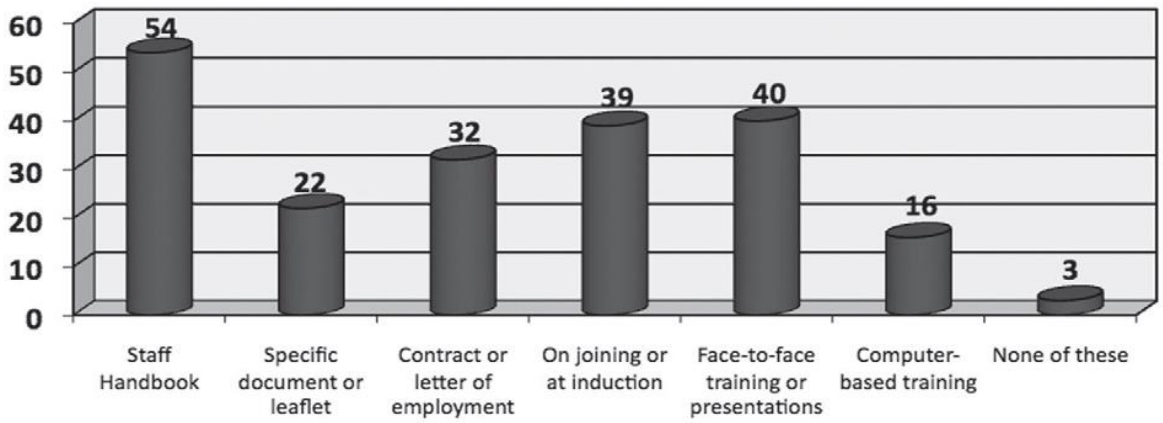


Figure 3.1: Information Security Policy Communication Methods (BERR, 2008)

The key to success in awareness/training is to keep the messages relevant and consistent, while varying the delivery mechanisms in order to retain the recipients' interest. Both the delivery mechanism and the risk areas may change as the information risk profile changes. The channels of communication, as depicted in Figure 3.2, represent either written or verbal methods. Verbal and written communication methods are briefly discussed in the following sub-sections.

3.8.1.1 Verbal

A common form of verbal communication used in raising awareness is presentations/training with the common method used being a lunch and learn. When a lunch and learn is held, the presenter usually prepares a brief presentation for communicating to the group. According to Bacik (2008), the knowledge of the audience and the structure of a lunch and learn session enable the information security team to be able to present the session in three ways:

- **Tell and sell** – This is most effective for new employees and involves the presenter lecturing the audience on what is being implemented and trying to sell the concept to the audience. In such instances the presenter may expect defensive reactions or require the audience's acceptance of the concept.
- **Tell and listen –** This is an effective method when presenting a new topic or implementation. The presenter introduces the new concepts and then asks for feedback from the audience as to how to improve or make the implementation easier, for example, addressing a joint business requirement.

- **Fulfilling the business requirement** – This method is effective for formal implementations where the goal is to inform the audience why they need to comply with the information security policy architecture document, what they need to do and the results of compliance.

3.8.1.2. Written

Specific Document/Leaflet/Memo

When memos are used to communicate, the following questions should be asked and answered by the memo:

- What is the main message to be disseminated and what is the tone that will be used?
- Does the first paragraph contain all the key information?
- What do we want the group to remember and take action on from this memo?
- Are the statements convincing and feasible, and what do we want the group to do?
- What other risks are not included in this memo?
- Is the English used simple and straight forward?
- Has the memo been proofread before dissemination?

(i) Employee Handbook

The employee handbook is usually one of the items that a new staff member receives on his/her first day. However, it is often simply packed away and forgotten about. The employee handbook is a static document until there is a major change within the organisation, such as an enterprise acquisition or divestiture (Bacik, 2008). Thus, it is not possible for information security policy architecture to reside within an employee handbook because it is a living architecture document and it changes depending on the enterprise growth.

(ii) Intranet

The information security website, like the employee handbook, may become static if not maintained properly. Thus, it needs to be kept dynamic by updating it regularly

(Bacik, 2008). The information security Intranet site should keep all staff up to date with information on protecting the assets of the organisation, announcements of information security projects, tips and tricks for the home networking environment, and for becoming acquainted with the information security team.

(iii) Computer based training (e-training/e-learning)

Traditional classroom training is declining as a result of both the increased costs as well as the increasing popularity of e-learning (Gallagher & Sixsmith, 2014). The information security team must to assess which employees are being targeted for awareness training and design the best method to access these employees. In addition, the information security team needs to develop flexible and responsive sessions for the enterprise environment. Informal training must be both relevant and immediate, possibly using the prevailing work environment. The e-training sessions should be short and valuable so employees are able to become involved but without taking time away from enterprise projects.

The most common training methods used in e-communities include frequently asked questions, message boards with moderators, websites and chat rooms (Gallagher & Sixsmith, 2014). Although many organisations are aware of these options for projects they have not extended them to the information security awareness environment. Super users and subject matter experts may assist in keeping the material responsive, relevant and current.

Another method promoting e-learning is ‘brown bag’ lunches or ‘meet the experts’. ‘Meet the experts’ permits staff members to ask questions on how information security pertains to their work environment or to ask for a more detailed explanation of the existing information security policy architecture. The “brown bag” lunches and “meet the expert” sessions also enable the information security team to mentor employees, thus helping them to become more familiar with the information security team and also more comfortable with the information security policy architecture.

(iv) Informal Methods

Johnson (2006) identified useful and effective methods communicating information security awareness in terms of promotional and informational methods. These are listed in Figure 3.2.

Promotional Methods

- Events/fairs
- Screen savers
- Banners on the intranet
- Hyperlinks from the intranet home page to the security page
- Articles in the internal publication
- Posters
- Puzzles and games
- Pre-printed note pads or sticky notes
- T-shirts
- Mugs and cups
- Mouse pads
- Stickers

Enforcing Methods

- Underwriting security principles
- Confidentiality agreements
- Required awareness exam or test
- Disciplinary actions for non-compliance
- Inclusion in annual evaluations or promotion criteria
- Rewarding mechanisms

Educational/Interactive Methods

- Slide presentations
- Training
- Brief targeted sessions
- Online learning modules
- Demonstrations
- Videos
- Workshops

Informational Methods

- Leaflets
- Short articles or news stories
- Intranet security web site postings
- E-mail warnings
- Information security guides
- Tips-of-the-month
- Flash cards
- Newsletters

Figure 3.2: Information Security Communication Methods (Johnson, 2006)

Kajzer, D'Arcy, Crowell, Striegel and Van Bruggen (2014) and Albrechtsen (2007) encourage similar informal methods that include brief newsletter articles, quick notes, lunch meetings, discussion groups, screen savers, posters, and physical reminders such as mouse pads, pens, tension squeeze balls and games.

3.8.2. Barriers to Effective Communication

The main aim of an employee information security awareness campaign is to make sure that the organisation's information security policy is well understood and followed by all employees in the organisation. The audience (employees) tends to check the credentials of the information security personnel before accepting the information communicated (Bacik, 2008; Chipperfield & Furnell, 2010). It is essential that the members of the team are in possession of acceptable credentials.

Credentials do not necessarily mean a list of certifications after their names and may include “I have been actively participating in the industry and community for years”.

According to Bacik (2008), whether verbal or written communication is used, the following should be avoided:

- Slang or local dialect words
- Word associations that have different meanings for different people
- Emphasis or specifying certain words
- Incorrect or inappropriate use of words and phrases
- Omitting vital background information and assuming the audience possesses certain knowledge
- Homonyms or words with the same spelling and sounds but which have different meanings, for example, *their* or *there*

Before the message is communicated to employees, it is important to take time to consider whether an employee who receives the message will be able to understand what the information security team is trying to communicate as the information security team relies on the employee’s perception or interpretation of the message communicated.

3.9. From Information Security Knowledge to Information Security Compliance

A summary of the way in which information security awareness ultimately turns into to positive information security compliance is depicted in Figure 3.3.

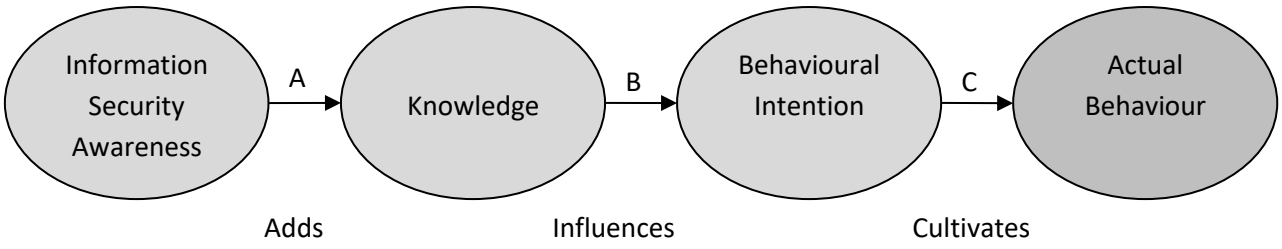


Figure 3.3: The Transition from Information Security Awareness to Information Security Compliance

Figure 3.3 depicts the general conception of the way in which awareness should lead to a positive actual behaviour (compliance) in a perfect world. However, links A, B and C are prone to weaknesses and conversion may not be as expected. For example, a badly communicated awareness campaign may fail to pass valuable knowledge onto the employees, thereby causing a weakness at A. In addition, the knowledge acquired may not be practical enough to bring about a change in behavioural intentions, hence causing a weakness at B. Intentions are self-proclaimed. The employee may respond with an expected and acceptable answer but behave differently, thus causing a weakness at C. This study focused on the weakness at C.

Research shows that intentions are an important but insufficient prerequisite for successful behaviour (Bhattacherjee & Sanford, 2009). This phenomenon has been labelled the *intention-behaviour gap* (Sheeran, 2002). In the TPB, Ajzen (1998) tried to remedy the limitations that exist in the relationship between intention and behaviour, and added perceived behavioural control to the model. However, despite the effort, there are still limitations in the relationship between intention and behaviour.

Psychologists Ouellette and Wood (1998) tend to believe that past behaviours guide future behaviours. They suggest that well-practised behaviours recur because they become part of the employees' culture and, alternately, when behaviours are not well learnt, employees tend to be more conscious when making decisions to initiate and carry out such behaviour. This study agrees that these relations between past behaviour and future behaviour are substantiated. However, in terms of information security compliance assessment, past post awareness and training behaviours only should be measured otherwise the security status and behaviour prediction may be inaccurate.

3.9.1. Intention-Behaviour Relations

There are, nevertheless, several problems which may arise when making inferences about causation on the basis of correlational studies. Firstly, many correlational studies use cross-sectional designs that render reports of intention and behaviour liable to consistency or self-presentational biases. These biases may inflate estimates of the strength of the relationship between intention and behaviour (Czellar, 2006) Secondly, and more seriously, is the problem that cross-sectional studies are not able to rule out the possibility that behaviour caused intention. For example, an employee may assume his/her intention to run a virus scan on the basis of the number of times he/she ran it the previous month through a process of self-perception (Bem, 1972). Thus, behaviour may be the cause of the reported intention rather than vice versa.

3.9.2. Problems Associated With the Conversion of Intention into Behaviour

(i.) **Job relatedness.** This dimension refers to whether an employee's behaviour is related to his/her job. In view of the fact that employees use ICT in an organisational setting, job-relatedness may be a key factor in their making a judgment as to whether the behaviour in question is appropriate. For example, copying sensitive organisational data onto a mobile data storage device may be done for work reasons, whereas surfing the internet for nonbusiness purposes is likely to be a completely different matter from the employers' standpoint.

(ii.) **Expertise.** This dimension refers to the degree of ICT knowledge and skills that an employee would require in order to perform the behaviour in question (Stanton et al., 2005). For example, hacking into a computer or cracking passwords would require higher levels of technical knowledge and skills as compared to writing down and posting a password on a monitor. This dimension is also related to the roles that employees play in the organisational setting. End users typically focus on using ICT to achieve

business objectives while IT people, on the other hand, focus on the management of systems and network. The differences in their roles may, therefore, contribute to differences in their understandings of security issues.

(iii.) **Consequence.** This dimension refers to whether an employee's behaviour will cause direct damage or pose risks to the organisation. Direct damage may be more salient to employees because it is directly observable or may be reasonably expected. Risks, on the other hand may not materialise and there is always the chance that there will be no damage at all. For example, running a known virus on a computer will cause damage to both the system and the data. However, opening a suspicious email that may contain a virus is different in that there is a risk of causing damage. In other words, there is an "uncertainty" in the latter case in terms of possible consequence.

3.10. Testing for the Relationship between Intention and Behaviour

In order to test the causal impact of intention on behaviour it is necessary to change intention and observe whether there is a corresponding change in behaviour. In an ideal world a 50% increase in intention strength should also produce a 50% increase in the subsequent behaviour if there is a direct relation between intention and behaviour. Several studies have manipulated behavioural intentions in this way and examined changes in the subsequent behaviours. For example, Brubaker and Fowler (1990) used a persuasive message based on the TPB to encourage men to perform a testicular self-examination (TSE).

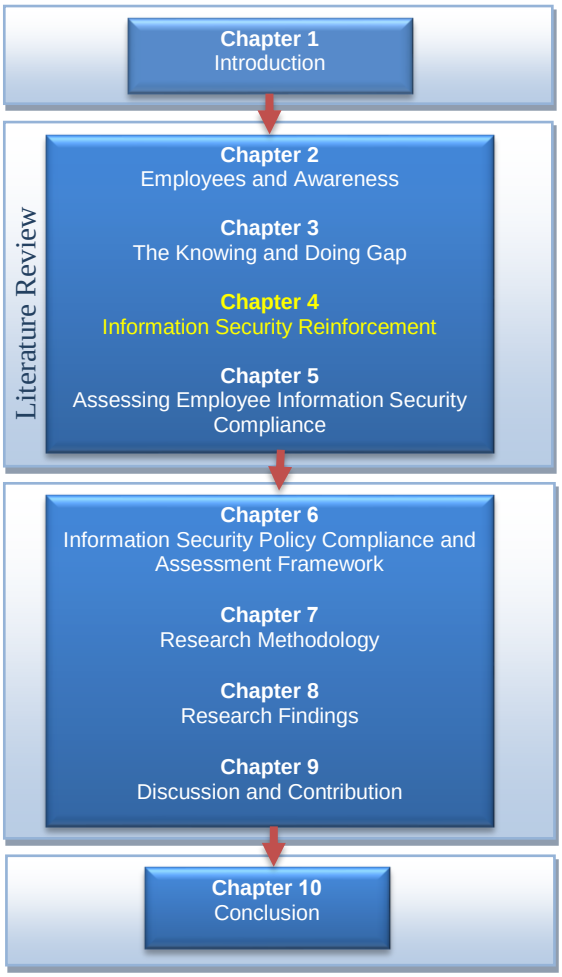
At the theoretical level several theories of attitude-behaviour relations, models of health behaviour and goal theories assume that changing intentions will change behaviour. Thus, estimating the size of the intention-behaviour effects enables a critical test of these theories. Estimates of effect size may illuminate whether the concept of intention is required in order to understand the process of behavioural change, whether additional concepts are needed, or whether researchers need to

look to other constructs to understand behaviour change. At the applied level numerous surveys have been conducted to establish the factors that should be targeted by interventions in order to change behavioural intentions (e.g. Kruger & Kearney, 2006; Jayasingh & Eze, 2015; Mtebe & Raisamo, 2014; Ngoqo & Flowerday, 2015). Moreover, these interventions deem intention to be a valid outcome because it is assumed that intention change will be translated into behaviour change. Thus, a substantial proportion of intervention research rests on the untested assumption that intentions cause behaviour.

3.11. Conclusion

Although awareness initiatives represent an acceptable solution to employees' naïve insecurities, this chapter highlighted the weaknesses that arises from inferring that knowledge will be translated into action. Thus, understanding the intention-behaviour gap, its causes and effects are important for both theoretical and practical reasons. Theoretically, understanding this gap helps both to reconcile the various findings in the empirical literature on the strength of this association and to re-evaluate the use of intention as a reasonable proxy for actual IT usage behaviours. Furthermore, this understanding may also advance the existing knowledge base of ICT usage by helping to delineate the boundary conditions beyond which current intention-based theories are less helpful in predicting information security compliance. From a practical standpoint, this gap may help to explain why organisational intervention plans which are designed to promote compliance (e.g. awareness programmes) are sometimes not very successful in achieving compliance. In addition, understanding the underlying factors causing this gap may help managers to design intervention plans that would help to bridge this gap or, at least, mitigate its potential effects. The next chapter focuses on information security motivation/reinforcement.

CHAPTER 4 - INFORMATION SECURITY MOTIVATION AND REINFORCEMENT



Chapter 4:

This chapter analyses and classifies employee behaviour in respect of information security and discusses the possible causes of the intention and behaviour gap. The chapter then goes on to discuss compliance persuasion techniques (push and pull). The chapter also focuses on employee issues in respect of information security compliance. Finally, the chapter explores the indications of both compliance and noncompliance.

4.1. Introduction

The success or failure of an organisation's information security initiative effectively depends on the behaviours of its employees (Peltier, 2005). Their compliance and good security practice, as detailed in the information security policies, are the best ways in which to minimise information breaches. However, such "good practice" needs to be reinforced to ensure that the employees actually behave as they are mandated to do.

Although leading information security behavioural theories such as the Theories of Reasoned Action and Planned Behaviour (Ajzen, 1991; Ajzen & Fishbein, 1985), and Protection Motivation Theory (Rogers, 1983) interpret intentions as the most immediate and important predictor of behaviour, these theories do not articulate the way in which intentions drive behaviour. Understanding the mechanisms that determine the strength of intention-behaviour relations is, however, important given that intentions generally explain 20 to 30% only of the variance in behaviour. The previous chapters highlighted the gap between knowing and doing while this chapter discusses the causes of the gap and possible solutions to it.

This research study sought to supplement behavioural theories with deterrence theories as a possible solution to motivate/reinforce compliance. Drawing on various deterrence theories research in social psychology, it is possible to observe a relationship between penalties/rewards and behaviour and, thus, to suggest that the intention-behaviour association may hold for employees fearing punishment or for employees attracted by the rewards associated with good behaviours.

4.2. Classification of Behaviour

The Cambridge English dictionary defines behaviour as the way that a person behaves in a particular situation or under particular conditions. Behaviours are usually classified as good, neutral or bad. This study adapts Parsons, McCormac, Butavicius, Pattinson and Jerram's (2014) classification of behaviour pointing out the study's information security focus area (as shown in Table 4.1).

Table 4.1: Classification of Behaviour (adapted from Parsons et al., 2014)

Focus area	Good behaviours (Deliberate)	Neutral behaviours (Accidental)	Bad behaviours (Deliberate)
Password management	Always logging off when computer unattended	Sharing usernames and passwords with spouses and/or colleagues	Hacking into people's accounts
Email use	Refusing email attachments from unknown sources	Opening unsolicited email attachments	Creating and sending Spam Email
Internet use	Using only authorised software	Accessing dubious websites	Downloading video content to a work computer via peer-to-peer file sharing
Social networking site (SNS) use	Not accessing social networking websites during work time	Not considering the negative consequences before posting on a SNS	Posting sensitive information about the workplace on social networking sites
Incident reporting	Being vigilant in recognising and approaching unauthorised personnel	Not reporting security incidents	Giving unauthorised personnel access to authorised precincts
Bring your own device (BYOD)	Ensuring your device is always scanned and clean of viruses	Lending your computer with work related information saved on it to a friend.	Configuring a virtual tunnel that gives access to company blocked web pages
Information handling	Shredding or destroying sensitive documents that need to be disposed	Leaving DVDs or documents that contain sensitive information on a work desk overnight	Writing and disseminating malicious code

4.3. What are The Possible Causes of this Intention-Behaviour Gap?

There are clearly many potential causes of this gap. According to the literature, potential general explanations of the causes of the gap include the following:

4.3.1 The Social Desirability Effect

This type of behaviour is one measurement factor that may influence the intention-behaviour relation (objective vs self-report). It has been found that self-report measures of behaviour may overestimate intention–behaviour associations because

of consistency, social desirability or memory biases (Krumpal, 2013; Kelly, Harpel, Fontes, Walters, & Murphy, 2017). Employees may report favourable intentions because they do not wish to portray themselves as at odds with either the organisational expectations or the researcher conducting a study (Bhattacherjee & Sanford, 2009). Hence, their actual behaviour may be different from the intentions stated if the employees concerned are truly opposed to the expected behaviour.

4.3.2. Volitional Control

Several theories predict that greater perceived or actual control over behaviours should be associated with improved prediction of behaviour by intention (e.g. TPB, Theory of Reasoned Action and Behaviourism Theory). Thus, employees' perceived behavioural control or self-efficacy is assessed. The type of intention measure may also index control perceptions. Whereas behavioural intention refers to what one intends to do (e.g. Do you intend to run a virus scan this month?), behavioural expectation (BE) refers to self-predictions about what one is likely to do (e.g. How likely is it that you will run an antivirus scan this month?) (Sheeran & Webb, 2016). Measures of BE are thought to encompass an employee's perceptions of factors that may either facilitate or impede the performance of a behaviour. However, evidence indicates that people may overestimate the amount of control they possess over their behaviours (Langer, 1975; Sheeran, Trafimow, & Armitage, 2003). For this reason, two objective assessments of volitional control are taken: (a) effect sizes are computed for interventions that change both intentions and self-efficacy and for interventions that change intention only, and (b) independent raters are asked to assess the degree of control each sample is likely to have over the performance of the focal behaviours (Sheeran & Webb, 2016).

4.3.3. Analysis of Reasoned Actions versus Social Reactions

This analysis implies that intentions should better predict information security protective-behaviours (e.g. virus scans, encrypting sensitive emails) as compared to information security-risk behaviours, especially risky behaviours that are performed in social contexts and involve clear images of the type of person who engages in the

behaviour, e.g., disabling the antivirus to make a computer perform fast or pirate software downloads. The reason for this is that information security protective-behaviours are assumed to be under intentional control whereas risky behaviours are often determined more by what the person is willing to do in risk-conducive circumstances than by intention. Thus, whether or not the focal behaviour has the potential to engender social reaction is assessed.

4.3.4. Habitual Control

According to Neal, Wood & Quinn (2006), behaviours that are performed frequently in stable contexts support the development of habits and, thus, the impact of intention on behaviour is attenuated. A meta-analysis conducted by Ouellette and Wood (1998) showed that, when behaviour is practised repeatedly and the context of performance is stable, past behaviour is a better predictor of future behaviour as compared to intention, whereas the reverse was true when behaviours were performed infrequently in unstable contexts.

Similarly, Verplanken, Aarts, Van Knippenberg, and Moonen (1998) found that with regard to the interaction between habit and intention, intentions were only significantly related to behaviour when the habit strength was weak. On the other hand, when the participants possessed moderate or strong habits, their intentions had little influence on their subsequent behaviour (Schwab & Wolf, 2011; Klockner, Matthies, & Hunecke, 2003). However, Ajzen (2002) and Cushman and Morris (2015) had a different view. Thus, whether behaviours have the potential to be controlled by habit may be an important moderator in intention-behaviour relations.

4.3.5. Attitude Strength

The literature also highglights a potential theoretical explanation of the intention-behaviour gap as being derived from the ‘attitude strength’ concept in social psychology (Bhattacherjee & Sanford, 2009; Kruger & Kearney, 2006). This line of research suggests that people with ‘strong’ attitudes demonstrate a stronger

association between attitudes and behaviour, whereas those with ‘weak’ attitudes often demonstrate a weaker association.

In view of the fact that intention represents the conative dimension of attitude (Breckler 1984), this reasoning may be extended to explain the intention-behaviour gap. Although people may exhibit differential strengths in their voting, pro-choice or anti-war attitudes, rarely will they demonstrate equivalent strengths in their attitudes towards information security compliance. According to Bhattacherjee and Sanford (2009), employees with strong attitudes towards information security usually comply better with policies and invest more time and effort in learning how to protect the information asset better as compared to those with weak attitudes who may initially buy into the information security initiatives but lack the commitment to comply over the long term and, thus, they often expose the organisation to numerous risks.

4.3.6. Time Interval

The time interval refers to the time interval between the measure of intention and behaviour. Ajzen (Ajzen, 1985) repeatedly asserted that, to obtain accurate prediction of behaviour, intention must be measured as close in time as possible to the measure of behaviour. The reason for this is that intervening events (e.g. new information) may produce changes in intentions so that that the original measure may no longer predict the behaviour. Meta-analysis supports the notion that temporal contiguity affects the extent to which intentions predict behaviour. Sheeran and Orbell (1998) found a significant negative correlation between time interval (measured in weeks) and the strength of the intention-behaviour association.

4.4. Compliance Persuasion Techniques

It is appropriate to consider various ways of shaping employee behaviour by drawing on knowledge from the management domain. The widely cited style in this context is Berlew and Harrison’s (1978) categorisation of the ‘push’ and ‘pull’ styles of influencing behaviour. Table 4.2 presents a summary of the ‘push’ and ‘pull’ styles.

Table 4.2: Push and Pull Styles (Berlew & Harrison, 1985, in Chipperfield & Furnell, 2010)

Pull	***Participation and trust***	Focuses on the involvement of others in the decision-making process as part of a more open approach of mutual trust collaboration.
	Common vision	Presents a view of the ideal outcome, emphasising the potential for collective benefit together with the need for an associated group effort and commitment to the outcome.
Push	***Reward and punishment***	A top-down approach based on the use of pressures and incentives in order to encourage compliance with defined expectations.
	Assertive persuasion	Involves the use of facts, logic and evidence in order to provide a persuasive case for the desired action.

4.4.1. Pull Technique

Pull approaches are by far the most common styles used in the traditional promotion of security (Chipperfield & Furnell, 2010). For example, techniques around common vision may provide a useful foundation for understanding why security is needed and what the management of the organisation feel about it. Many will often buy into the notion on this basis.

A common vision may assist in establishing an overall security culture within the organisation and, in that sense, a common vision is necessary as part of ensuring that this happens. Looking at the 'pull' styles, approaches that hinge on participation and trust are also very relevant in the context of promoting the broad security message and may also be valuable at the level of engaging individual employees or small groups (Chipperfield & Furnell, 2010). Awareness campaigns and training represent a good form of 'pull' techniques.

'Pull' styles may also be effective for communicating expected behaviours and achieving positive behavioural intention. However, other styles may also be required

to take employees through the conversion of intention to their actually behaving in accordance with the requirements (Chipperfield & Furnell, 2010).

4.4.2. Push Technique

For example, techniques around assertive persuasion may provide a useful fouundation for understanding why security is needed and many will, at least, recognise the issue from this basis. The use of reward and punishment may create a framework within which the organisation is able to formally lay out its expectations to the staff. Examples of 'push' styles are presented in Table 4.3.

Table 4.3: Examples of push technique (reinforcing methods)

Reinforcing Methods
• Underwriting security principles • Confidentiality agreements • Required awareness assessment • Disciplinary actions for non-compliance • Inclusion in annual evaluations or promotion criteria • Rewarding mechanisms

4.4.2.1. Promotion of Benefits (Push-Assertive Persuasion)

The promotion of benefits entails being explicit about the direct benefits of security to the employee, for example, what it means to both them as individuals and the organisation. The benefits may be promoted through a series of campaigns such as the 'ABC' of security or 'Did you know?' posters.

Initial articulation by the organisation may be necessary to establish clarity around the tangible benefits of security before such a campaign is developed. However, sometimes even the organisation itself may find it difficult to identify the tangible benefits of security (Chipperfield & Furnell, 2010).

4.4.2.2. Scare Tactics (Push-Assertive Persuasion)

Scare tactics may be used as part of a broader promotional campaign. However, they should be used sparingly. It is easy to fall back on the negative images of not using security and (to a degree) scare tactics already have an established role in security (through their relationship with techniques such as penetration testing). However, it be borne in mind that that such tactics may cause inadvertent damage by alienating the target audience. Scare tactics work for a short period but they are not sustainable.

4.4.2.3. Internal Reward Process (Push-Reward and Punishment)

This mechanism uses an internal scheme to reward the acceptance of a security update or activity. It may be compared to a shopping loyalty reward card and, as such, gives the user with an incentive to support the company initiative. This mechanism may involve simple 'prizes' such as a unique screensaver or background or even a floating trophy to display on the desk.

4.5. Identified Employee Issues With Respect to Information Security Compliance

The literature review on existing information security policy implementations identified a number of issues. The issues presented in this section are not limited to the policy documents themselves but include issues which impact on both policy effectiveness and on the information security awareness of the employees in an organisation. Talbot and Woodward (2009) summarised these issues as the way in which user awareness represents a significant challenge in the security domain, with the human factor, ultimately, being the element that is exploited in a variety of attack scenarios. His findings may be classified as follows.

4.5.1. A Culture of Ignoring Policies

The history and the way in which the organisation has implemented policies may have resulted in a culture within the organisation in terms of which employees ignore those policies with which they do not wish to comply. This is a major hurdle which must be addressed before any policy implementation may be effective (Talbot &

Woodward, 2009). A number of information security policies are often scoffed at when they are ready for implementation. Comments such as “Who cares about the policy, you can’t enforce it” are commonplace within organisations with the majority of employees viewing these policies as a means of disciplining them or hindering their development and operational advancement.

4.5.2. Minimal Awareness of Policies

Most organisations display their corporate polices both on the intranet and in their contracts of employment. Although part of these policies include the information security policy it would appear that employees are unaware of them. An awareness of the contents of relevant policies is usually non-existent. The mandatory signing of policies for employees on induction does not ensure that the employees have read and understood the contents of the document (Johnson, 2006) while, for those who have read it, refresher courses on the policy’s contents are of great importance.

4.5.3. Minimal Policy Enforcement

Policies, especially information security related policies, are often ignored if there is a chance they may impact on the quick and simple implementation of ICT services (Talbot & Woodward, 2009). In instances in which policy breaches have been brought to the attention of management claims are often that it is either not possible for the policy to be enforced, or that the policy should be rewritten. In addition, policy enforcement is often ad hoc and not enforced uniformly across the whole organisation (Talbot & Woodward, 2009).

4.5.4. No Formal Non-Compliance Reporting

There is often no formal reporting of policy breaches and non-compliance with employees not being aware of what their responsibilities are, how they should report issues and to whom they should report them (Talbot & Woodward, 2009). As a result several issues are not referred to the appropriate bodies while the information security teams are often not involved. A number of issues eventually come to the attention of the team long after the event and, thus, long after any action should or could have been taken.

4.5.5. Apparent Inconsistent Enforcement across the Whole Organisation

There are a number of examples in organisations where employees are aware of their colleagues being dismissed for activities which appear to be in breach of the user policy although similar cases involving management have resulted only in minor disciplinary warnings (Talbot & Woodward, 2009). However, this apparent ad-hoc and non-consistent enforcement may have a negative effect the overall realisation of good security behaviours.

4.6. Compliance vs Non-Compliance

Table 4.4 presents the stages between the two extremes, namely, information security compliance and information security non-compliance.

Table 4.4: Levels of Security Compliance Based Upon Individual Behaviours (Adapted from Furnell and Thompson, 2009)

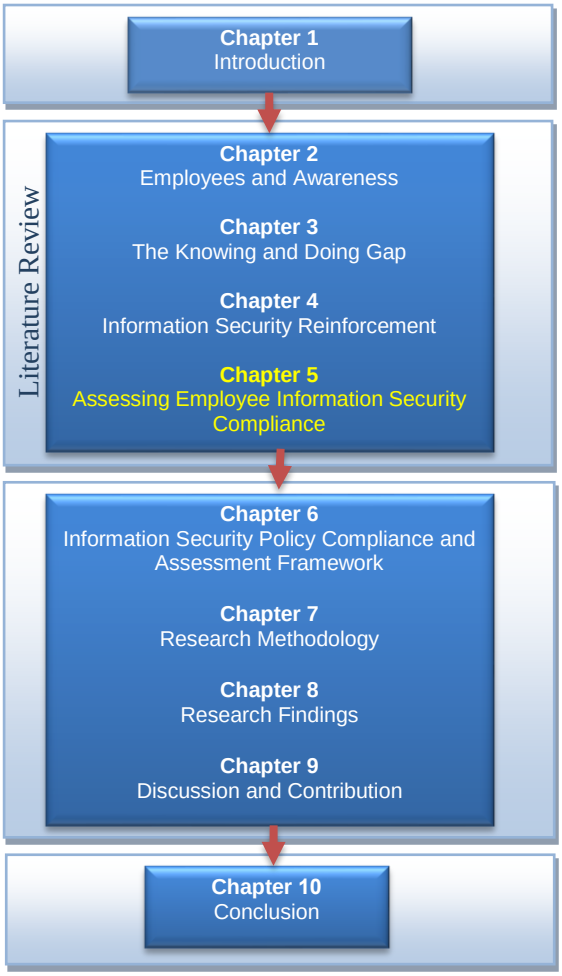
Compliance	Culture	The ideal state in which security is implicitly part of the employees' natural behaviour
	Commitment	Security is not a natural part of behaviour but, if provided with appropriate guidance/leadership, then the employees accept the need for it to be associated with natural behaviour.
	Obedience	Employees may not buy into the principle but are forced to comply through the appropriate authority.
	Awareness	Employees are aware of their role in information security but are not yet necessarily fully complying with the associated practices or behaviour.
Non-Compliance	Ignorance	Employees remain unaware of security issues and, thus, they may introduce inadvertent adverse effects.
	Apathy	Employees are aware of their role in protecting information assets but are not motivated to adhere to sound information security practices.
	Resistance	Employees passively work against security by opposing those practices with which they do not agree.
	Disobedience	Employees actively work against security, with insider abusers intentionally breaking the rules and circumventing controls

4.7. Conclusion

The discussion in this chapter highlighted the true extent of the challenges regarding the raising of awareness against the paucity of related secure behaviours. Although it is widely known that security may be promoted in a variety of different ways, there seems to be little recognition of the reasons why it should, in fact, be promoted. Promoting security should not just involve the act of ticking it off the to-do list and every effort should be made to ensure that it is targeted in an effective way.

The information security message must be personalised and shaped to fit the roles of the employees, their levels of interest. In addition, it should be such that they feel comfortable engaging with it. It is always good practice after the messages have been crafted and communicated to ensure that they have been correctly understood and are, in fact, having the desired effect. This may seem obvious but literature, nonetheless, suggests that there are many organisations that do not check this. For example, the ENISA (2007) survey suggested that 42% of organisations compare the level of information security awareness pre and then post the implementation of the programme. After the awareness and reinforcement initiatives have been completed, it is is essential to ascertain whether the desired compliance has been achieved and, hence, some form of assessment is necessary. The next section discusses ‘how’ to assess such initiatives.

CHAPTER 5 - ASSESSING EMPLOYEE INFORMATION SECURITY COMPLIANCE



Chapter 5:

This chapter analyses the methods that may be used to assess information security compliance. Thus, the chapter attempts to addresses the problem of "what" to assess and "how" to assess it. It then goes to discuss the method used to analyse the data which has been collected. The chapter also discusses the efficiency and effectiveness of information security compliance assessment methods.

5.1. Introduction

The need for information security awareness campaigns was discussed in the preceding chapters. However, how does an organisation realise that it actually needs to raise security awareness and how does it know which topics should be addressed? If the main aim of information security awareness campaigns is to motivate compliance, the following question then arises, namely, “How will the organisation know it has achieved this?” This highlights the need to assess behavioural change and check whether the campaigns have resulted in improved compliance. Chapter 3 discussed the objectives of information security training. These objectives included enhancing the existing security knowledge so as to cultivate a positive attitude towards security, positive security behaviour and security compliance. These objectives represent the parameters against which compliance is usually assessed. As already stated compliance assessment does not constitute a tick in the regulatory box in order to provide evidence that everyone in the organisation has been through a security awareness ‘sheep dip’ but, rather, to ascertain whether the assessment has brought about behavioural change.

Without such assessments it is impossible to establish whether or not an appropriate return on the investment has been realised. In addition, assessment also plays an important part in enabling organisations to identify aspects in respect of in-depth training or reinforcement is required as well as aspects where it may be possible to spend less without adversely impacting on the security risk profile. Hinson (2006) argues that an organisation’s management cannot manage what it cannot assess and it cannot improve on what it cannot manage. This highlights that assessment of information security compliance is important both for its management and for improvements. Such assessments may also assist in setting up targets and deadlines.

The majority of academic surveys of ICT users have examine one component of information security only. For example, Dupuis, Crossler, and Endicott-Popovsky

(2016) assessed privacy; Allam et al. (2014) examined smartphone security awareness; Furnell, Jusoh, and Katsabas (2006) assessed user security knowledge within specific applications; Siponen et al. (2010) and Herath and Rao (2009) examined employee intention to comply with policy, and Stanton et al. (2005) surveyed password-related behaviours. However, the literature provides little evidence of studies that have attempted to determine the overall employee information security compliance.

This chapter firstly presents an overview of the frameworks which may be used for evaluating information security compliance, secondly, it identifies what should be measured and how it should be measured and, finally, it discusses methodologies for data analysis.

5.2. Assessing Information Security Compliance

Correlational studies show that awareness is associated with behaviour. However, the level of the relationship between the two is debatable. Figure 5.1 below illustrates the general inference that awareness increases knowledge, which increases the behavioural intention to comply which then leads to positive behaviour, for example, assessing either knowledge or behavioural intention and assuming the result equates to compliance (positive, actual behaviours).

Figure 5.1: From Awareness to Actual Behaviour

There are several problems associated with making inferences about causation on the basis of correlational studies. Firstly, several correlational studies use cross-sectional designs that render reports of intention and behaviour liable to either consistency or self-presentational biases. These biases may inflate estimates of the strength of the relationship between intention and behaviour (Kautonen, Gelderen & Fink, 2015). Secondly, and more seriously, is the problem that it is not possible for cross-sectional studies to rule out the possibility that behaviour caused intention. For

example, an employee may infer his/her intention to scan for viruses on the basis of the number of times he/she scanned for viruses in the preceding week through a process of self-perception (Bem, 1972). Thus, such behaviour may be the cause of the reported intention rather than the other way around. Thirdly, the path from behaviour to intention is precluded by the use of longitudinal designs that correlate measures of intention taken at one point in time with measures of behaviour taken at a later point in time (cross-lagged panel designs also take initial behaviour scores into account).

Different organisations adopt different methods to assess information security compliance. These methods include both quantitative and qualitative approaches. There is, however, no agreed upon method because of the complexity of identifying what to assess and how to assess it (Kruger & Kearney, 2006).

5.2.1. What to Assess

Deciding what to assess and how to measure it may be extremely problematic for information security professionals. However, the literature review revealed that there are a number of measures that may be effective in providing insights into the levels of information security compliance within organisations, as well as showing progress in such compliance when collated on an ongoing basis over a period of time.

The problem with regard to information security compliance assessment criteria is revealed by the absence of any consensus in terms of what to measure and how to measure it.

It is clear that the effective measurement of awareness involves measuring both behavioural intentions and actual behaviours. Table 1 summarises the suggestions for pertinent studies:

Table 5.1: A Summary of Approaches to Assessing Information Security

Author	Type of Behaviour Assessed	Assessment Criteria
Safa, Von Solms, and Furnell (2016)	Behavioural intention	Attachment, involvement, commitment, personal norms
Posey et al. (2014)	Behavioural intention	fear of sanctions, incentives, motivations, pride
Davis (2008)	Behavioural intention	Knowledge, behavioural intention.
ENISA (2007)	Actual behaviour	Process improvement, attack resistance, efficiency/effectiveness, internal protections
Payne (2010)	Behavioural intention	Metrics
Kruger & Kearney (2006)	Behavioural intention	Knowledge, attitude, behavioural intention
Chapple (2005)	Actual behaviours and behavioural intentions	Audits, lost productivity, user satisfaction, knowledge
Ouellette & Wood (1998)	Actual behaviour	Past behaviour to predict expected behaviour
Ajzen (1985)	Behavioural intention	Attitude, perception, subjective norms

5.2.1.1. Operational Measures: A Useful Starting Point

In many organisations the measurement of awareness and training begins and ends with operational measures (Hinson, 2006). This provides useful quantitative data such as:

• The number of employees trained

• The frequency of training

• Pass and fail rates for assessment tests

For those SMEs which carry out information security campaigns, the usual tool they use is classroom style teaching which lends itself to operational reporting. Typically, the learning style provides a range of reports showing completion rates, assessment scores, etc while some level of profiling by department, geography or other specific

criteria is also possible. This level of operational reporting may be particularly useful for the purposes of regulatory compliance or for internal or external auditing purposes. However, while measuring the type of quantitative data described above over a given period is a useful starting point which provides an indication of trends in the levels of information security awareness, it does not, necessarily, provide an indication of the effectiveness of training which is impacted upon by several, different internal and external factors. Nevertheless, it does enable meaningful conclusions to be drawn about the impact of awareness initiatives. At the very least the audience group is understood and the effectiveness of the awareness tools used is ascertained. When collated on a year on year basis this data may provide a useful internal benchmark showing the growing reach of awareness initiatives. However, in order to gain a more valuable insight into the penetration of information security throughout an organisation, this approach needs to be combined with qualitative performance data.

5.2.1.2. Performance Measures – The Combined Role of Attitudes, Knowledge and Behaviours

Once the basic discipline of routine and accurate reporting of operational measures has been established, a range of more in-depth performance measures should be considered. These measures focus on whether the observed trends in information security are directly related to the information security awareness training, and whether the training is having the desired effect in terms of both user behaviour and the organisational security culture (Hinson, 2006).

In deciding which performance metrics to capture, it is important to consider the key determinants of security behaviour. Kruger and Kearney (2006) highlight three dimensions that should be assessed, namely, what a person knows (knowledge); how the person feels about the topic (attitude); and what the person does (behaviour). Employees' attitudes towards information security are important because, unless they believe that information security is important, they are unlikely to work in a securely way, irrespective of how much they know about the security

requirements. Attitude also provides a sound indication about an employee's disposition to act. Knowledge is important because, even if a user believes security is important, he/she is not able to translate that intention into action without the necessary knowledge and understanding. Finally, no matter what individuals believe or know about information security, there will be no positive impact on security unless they behave in a secure fashion.

Thus, enhanced information security lies in the overlap of attitudes, knowledge and behaviour as represented in Figure 5.2. Consequently, these are the aspects that should be addressed in awareness campaigns and also the aspects that should be measured to evaluate whether awareness and training are having the desired effects (Kruger & Kearney, 2006).

Figure 5.2: Enhanced Security

5.2.2. How to Assess

Quantitative research methods such as conducting surveys and the validation of frameworks and questionnaires have been deployed with marked success in the information security discipline (Schlienger & Teufel, 2005; Siponen et al., 2009; Al Hogail, 2015; Woon, Tan, & Low, 2005).

The literature review showed that measuring such performance intangibles as attitudes, knowledge and behaviour is difficult. Nevertheless, there are a number of methods which may be used to measure these tangibles effectively. The most effective of these methods include assessment tests, surveys and interviews.

Figure 5.3 depicts the various evaluation and feedback mechanisms that may be used to assess information security compliance.

Figure 5.3: Evaluation and Feedback Techniques (Wilson & Hash, 2003)

5.2.2.1. Assessing Attitudes

1. **Questionnaires** are the best tool for eliciting information from large numbers of respondents. In addition, they enable the identification of broad trends (Hofstee, 2006). A typical way of approaching drawing up items for a questionnaire would be to use an agreement scale to allow the employees to indicate their degrees of agreement with statements on security, e.g. easy access to data is more important than protection against unlikely security breaches and viruses (strongly agree, agree, neutral, disagree, strongly disagree). A survey is a method that organisations may use to study information security behavioural content in general as well as the attitude and opinions (De Vaus, D. (2013) of employees about information security in particular. The survey should, however, be validated to ensure that the questionnaire assesses what it claims to assess, namely, information security knowledge, attitude and behaviour (De Vaus, 2013; DaViega & Eloff, 2010; Dhillon & Torkzadeh, 2006).

2. **Interviews** are an ideal method for collecting qualitative data. Through a series of open-ended questions interviews allow the employee both time and scope to discuss their opinions on information security issues.

Interviews are particularly useful for obtaining data about attributes which cannot easily be observed (e.g. feelings, emotions, and attitudes) (Hofstee, 2006).

5.2.2.2. Assessing Knowledge

The most reliable measure of employee knowledge is a well-designed *assessment test* (Kruger & Kearney, 2006). Many assessment tests are poorly constructed and, while they may measure knowledge, they often do not measure the appropriate knowledge. The questions in the assessment test should relate directly to the behavioural learning objectives as this helps to validate whether the employees understand the security behaviours that are required of them (Kruger & Kearney, 2006).

5.2.2.3. Assessing Behaviour

Meaningful indications of employee behaviour or intended behaviour may be captured from *survey* data. Behaviour as indicated in in surveys tends to constitute a reasonable indicator of actual behaviour (Kruger & Kearney, 2006). For example, the following question would provide a strong indicator of behaviour or intended behaviour: “I would never share my password with a colleague”.

5.2.2.4. Assessing Process Improvement

This approach assesses the effectiveness of an awareness campaign by focusing on the campaign activities i.e. measures of the effort put into the campaign. However, this approach does not directly assess whether or not the campaign has resulted in improved security. Possible performance indicators include:

- The extent of the development of security guidelines. For example, employees are able to assess how well the security guidelines address the main security risks or technology platforms;
- The extent to which the guidance is disseminated. Typical metrics include the number of leaflets distributed, visitors to the intranet site, or staff receiving awareness training;

- The efficiency of the awareness process. The normal measure is the cost of delivery, e.g. cost (in time and expenses) per employee trained;
- The relevance of the awareness material. A simple measure here is the frequency with which the material is updated; and
- The effectiveness of the deployment of the security guidelines. Surveys that ask employees whether they are aware of security guidelines and know which procedures to follow are one way in which to measure this.

The advantage of process improvement measures is that they are easy both to define and to gather. However, the disadvantage is that they provide indirect reassurance only as to whether the organisation is becoming any more secure as a result of the programme.

5.2.2.5. Assessing Internal Protections

This category focuses on the extent to which an individual is protected against potential threats. In other words, has the individual's awareness resulted in secure behaviour? Possible performance indicators include:

- The extent to which employees incorporate security into the development and acquisition of systems. This may be measured by reviewing a sample of business cases and requirements specifications;
- The extent to which employees protect their data files. Scanning tools may be used to ascertain this;
- The extent to which employees have allowed their systems to be infected by viruses or other malicious software. Anti-virus activities usually provide statistics on this; and
- The extent to which employees have allowed their systems to harbour inappropriate material (e.g. pornographic) or unauthorised software (e.g. pirated). There are specific scanning tools that may quickly measure this.

The advantage of these measures is that they provide direct evidence of employee behaviours and assess whether awareness is making the organisation more secure

while avoiding either hypotheses or extrapolation. In addition, existing audits (by internal or external auditors) may provide effective feedback here for free.

The disadvantage of these measures, however, is that any individual assessment is quite specific to the behaviour it is assessing. An awareness campaign often aims to change several behaviours and this may result in numerous potential metrics. Each metric, in turn, may require investment in scanning tools or audits. Nevertheless, a risk-based or rotational approach may help reduce the ongoing cost.

SMEs should therefore consider using a combination of the five approaches as blending the different measurements will enable them to build up a balanced awareness measurement. Decisions on security are usually based on the overall picture rather than on any single measure. Either retaining or increasing information security resources requires a justifying quantification of the awareness campaign. In the main this involves interrogating mainly four of the five approaches and omitting assessing process improvement due to time constraints as this requires the assessment of long period of times.

Although assessing the effectiveness of various efforts may be both costly and time consuming, it must, nevertheless, be done to ensure that the information is reaching the employees (Kruger & Kearney, 2006). A survey conducted by Richardson (2008) found that 32% of the respondents did not measure information awareness in their organisations. This was mainly because of the cost and the absence of a commonly agreed upon and understood standard measurement of the effectiveness of information security awareness and training. Assessing education and awareness is not always straightforward and, thus, creativity is vital (Russell, 2002). Whilst Hinson (2006) argues that it is possible to assess information security successfully, he also acknowledges the difficulties inherent in the measurement process. He cautions against assessing the wrong elements, subjectivity, absolute measurements, the cost

of measuring to organisations, the interdependencies between management and measurement, measuring process outcomes and the meaning of numbers.

5.2.3. Attack Resistance

This approach focuses on measuring the extent to which employees are resistant to a potential attack. Possible performance indicators include:

- The extent to which employees recognise attacks. This usually involves asking specific questions in an employee survey, quiz or computer-based test; and
- The extent to which employees 'fall prey' to attacks. Simulated attacks, such as emails containing executables or people telephoning to ask employees for their passwords, are helpful.

The advantage of attack resistance measures is that they provide some direct evidence of the actual state of employee awareness. In addition, they often play a useful role in impressing on senior management the need for investment in security awareness.

The main disadvantage of these measures is that there are potentially numerous attack scenarios and any individual measure will be quite specific to the scenario it is testing. It may also be relatively expensive to set up simulated tests. However, a risk-based approach may help to address these issues.

5.2.4. Efficiency and Effectiveness

This approach focuses on the actual experience of security incidents within the organisation. Possible performance indicators include:

- The extent of the security incidents arising from human behaviour. Typical metrics include the number and cost of such incidents. Some organisations also take into account the proportion of security incidents arising from human behaviour;
- The extent of downtime arising from human behaviour. This is of particular concern in sectors in which the availability of systems is critical; and

- The extent to which human behaviour caused the organisation's most severe incidents. Root cause analysis into the serious incidents provides this data. The measure is usually then expressed as a proportion of the total number of serious incidents.

The advantage of these measurements is twofold: firstly, the data may be gathered through the overall security incident monitoring that most information security groups conduct as a matter of course and, secondly, these results are usually of great interest to senior management. However, the disadvantage of these measurements is that they do not necessarily provide a true reflection of the prevailing security awareness. It is not just security awareness that determines whether incidents occur and the extent to which attacks actually occur is important. In the long term, however, the trend may be a good indicator of awareness although, in practice, organisations often take action based on individual incidents. This may not, however, be the most effective approach.

5.3. Data Analysis

Kruger and Kearney (2006) proposed using weighting for the purpose of data analysis. They proposed the weighting as depicted in Table 5.2. However, the weighting may be changed to meet different management demands.

Table 5.2: Awareness Importance Scale (Kruger & Kearney, 2006)

Dimensions	Weighting (%)
Knowledge	30
Attitude	20
Behaviour	50

Kruger and Kearney (2006) processed results and importance weights in a spreadsheet application, and output was finally presented in the form of graphs and awareness maps. Table 5.3 shows the scale they used to explain the level of awareness. Although they found this scale suitable for their application management could change the scale to suit its requirements.

Table 5.3: Awareness Level Measurement (Kruger & Kearney, 2006)

Awareness	Measurement (%)
Good	80-100
Average	60-79
Poor	59 and less

A primary responsibility of information security programmes is to raise user awareness of information security issues. A rudimentary training programme should minimally educate employees on critical issues. Measuring the effectiveness of this rudimentary training programme then provides an opportunity to ensure that employees are receiving the relevant information they require to carry out their jobs safely and effectively. These surveys assess the awareness of job-specific information security issues. For example, if employees are asked how often they think they should change their password and 75% report that they do not see the need the change passwords, then it may be necessary to emphasise good password behaviour in the information security awareness programme. Similarly, if they are asked about appropriate methods for transmitting confidential information to a business partner and 50% of them indicate that they believe that unencrypted e-mail is all that is required, this is a clear sign of a deficiency that needs to be corrected. High scores indicate an effective education programme. If employees are consistently making errors in the same areas, then the awareness programme is not addressing the correct aspects.

SMEs generally have a limited number of employees and, hence, random number generators may be used to select the employee to be assessed. This will avoid the selection of only those who play an active role in the organisation's information security as this may skew the results. In order to ensure optimal cooperation,

employees should be assured that the assessment is being conducted anonymously throughout the organisation with the aim of potentially adding resources to improve security awareness. It is essential that they do not feel as if they are being graded on a test or that their scores will be reported to management as this is a surefire way in which to compromise the participation rate.

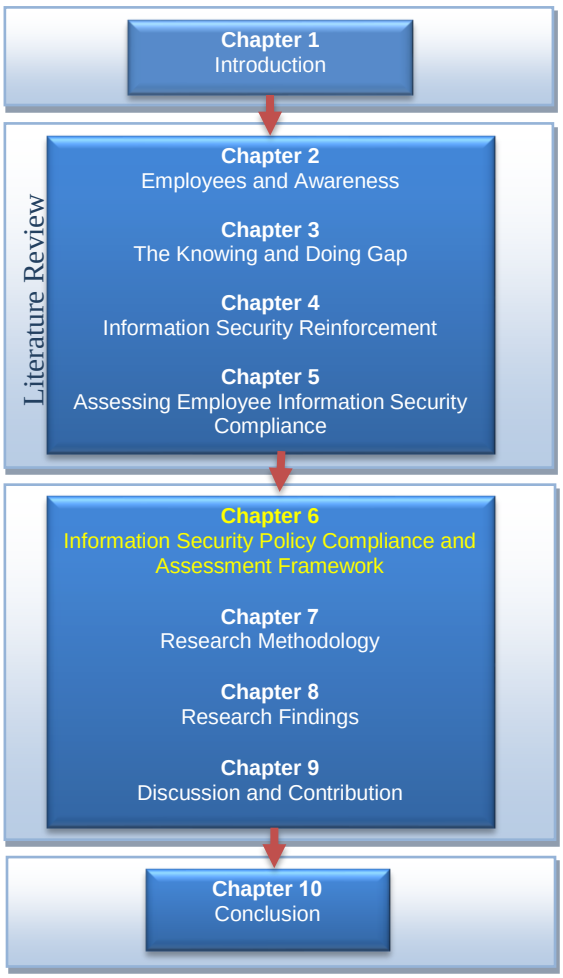
5.4. Conclusion

By its very nature, information security compliance is a critical aspect of any organisation. This chapter highlighted the tools and methods which may be used to assess the effectiveness of an organisation's information security awareness and training, thereby enabling the organisation to evaluate whether or not their information security awareness campaigns have resulted in a positive change in the knowledge, attitudes, behaviours and compliance of employees. By adopting a pragmatic approach and identifying reasonable and rational measures of employee behaviour, it is possible to evaluate the extent to which awareness activities have impacted on behaviour and, therefore, whether or not the initial training objectives have been realised.

After developing an instrument for assessing the information security compliance within an organisation, the results of the assessment assist in both validating the information security compliance component categories and ensuring a valid and reliable information security compliance assessment instrument. Corrective action plans may be deployed to help to minimise the threat that human behaviour poses to the protection of information assets.

Quantifying the success of information security efforts may result in additional resources while, at the very least, it may help in the formulation of accessible information security objectives for budgeting. Having reviewed the relevant literature in Chapters 2, 3, 4 and 5, the next chapter discusses the research methodology used in the study.

CHAPTER 6 - INFOMATION SECURITY POLICY COMPLIANCE AND ASSESSMENT FRAMEWORK



Chapter 6:

Information security models and frameworks are presented by researchers to guide organisations and to provide a structured approach when addressing issues relating to information security. This chapter discusses the proposed Information Security Policy Compliance Reinforcement and Assessment Framework which may be used to achieve employee information security compliance. The three models included in the framework are also discussed.

6.1. Introduction

An employee (insider) may expose an organisation's information assets to risk by making naïve mistakes (e.g. visiting malware infested websites, responding to phishing emails, using weak passwords, storing login credentials in unsecured locations, or giving out sensitive information over the telephone when exposed to social engineering techniques).

The primary role of awareness and training is to change employee behaviour towards compliance. In order to do this, the problem behaviour (also known as the target behaviour) and the desired behaviour (also known as the replacement behaviour) should be clearly defined (Van Nes, 2010), that is, they must be stated precisely in observable and assessable terms. When a behaviour is described in observable terms, it may easily be observed and documented. It may sound very logical to state that, in order for employees to play an effective role in the information security initiatives of an organisation, they need to be educated on the importance of their role in protecting information assets and they also need to know how to behave in order to fulfil this role. However, the literature reveals that this is not always the case. Accordingly, this chapter presents a framework with three models that should help to solve this problem. The chapter starts by detailing the theoretical foundation of the framework. Secondly, the proposed information security compliance assessment model, the employee behavioural model for behaviour motivation and reinforcement and theories underlying the models are discussed. Thirdly, motivation is provided for the choice of action research as the research approach used in the study. A summarised version of the development of the models is presented in Figure 6.1.

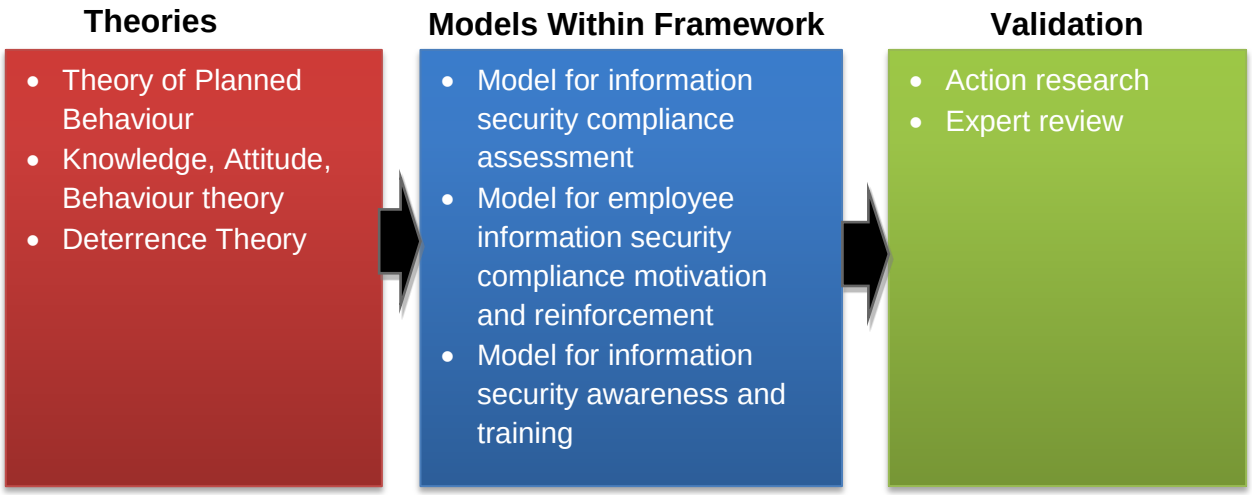


Figure 6.1: Methodology Summary

The rest of the chapter comprises the following: Firstly, the theoretical foundation of the framework is discussed, after which the three models of the framework are explored. Finally, the implementation method is discussed.

6.2. Theoretical foundation

Based on the problems discussed in the preceding chapters, this section proposes, explains and relates the TPB, KAB and DT to the proposed framework. The literature review revealed that previous works have used research frameworks that integrated the TPB, KAB and DT with other theories (e.g. Bulgurcu etal., 2010; Herath & Rao, 2009; Pahnila et al, 2007) but, nevertheless, the thorough review of literature in this area also revealed that no prior information security research had used all three theories in a single information security study. As depicted in Figure 6.2 these theories were linked in this study.

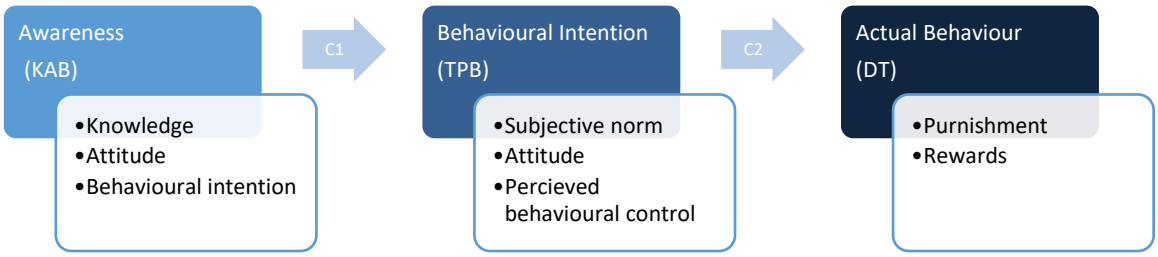


Figure 6.2: Theoretical Background

The TPB describes an individual's intention to perform a given behaviour over which the individual has incomplete volitional control. The TPB has been used as a framework for several studies in the information systems and information security fields. The TPB suggests that intentions are highly influenced by individuals' attitudes toward the behaviour in question, subjective norms and the perceived behavioural control surrounding the performance of the behaviour (Al-Omari et al., 2012). These intentions explain a high percentage of the variance in the actual behaviour. However, the theory formulated in this study postulates that intentions are expected to capture the motivational factors that influence both the behaviour and the amount of planned effort that will be exerted in order to perform the behaviour.

In order to address the compliance concern, various strategies for effective security compliance reinforcement were proposed. Drawing on the Deterrence Theory (DT), scholars usually advocate the negative enforcement strategy, namely, punishment. The DT proposes that, as the certainty and severity of punishment increase, unwanted behaviours are deterred. However, borrowing from theories in the organisational literature, some scholars support the positive enforcement strategy, namely, reward, arguing that reward provides necessary incentive and motivation for compliance and that reward combined with sanction is one of the important factors that may influence individual employees' rational cost–benefit assessment of compliance vis-à-vis noncompliance behaviours.

From a control perspective, both reward and punishment are control mechanisms which may be used to achieve organisational goals. However, in order to be effective, it is essential that such control mechanisms tie into the certainty of how often those control mechanisms are enforced or materialise. Certainty of control, referring to the probability of the enforcement strategy materialising, has been proved to be an influential factor that may contribute to the effectiveness of the enforcement strategy information security compliance (Siponen et al., 2009; Bulgurcu et al., 2010; Hu, Xu, Dinev, & Ling, 2011; Arage, Belanger & Beshah, 2015). However, to the best of the

researcher's knowledge, no prior studies in information systems have examined the interactive effects between punishment and reward and used this to motivate/re-enforce compliance.

6.2.1. Theory of Planned Behaviour (TPB)

The TPB is an extension of the theory of reasoned action (TRA) (Ajzen & Fishbein, 1985) and was developed by Fishbein and Ajzen (1975). It states that people's behavioural intentions are influenced by both attitude and subjective norms.

According to the literature, the TPB model has been verified empirically in psychology, marketing, medicine, pharmaceuticals, recycling, internet abuse, e-commerce adoption and information security (Ajzen 1991; Kautonen, Van Gelderen & Tornikoski, 2013; Cooke, Dahdah, Norman & French, 2016; Paviou & Fygenson, 2006; Chan & Bishop, 2013). TPB posits that employee behaviour is driven by behavioural intentions, where behavioural intentions are a function of the employee's attitude toward the behaviour, the subjective norms surrounding the performance of the behaviour, and the employee's perception of the ease with which the behaviour may be performed (behavioural control) (Ajzen, 1991).

According to TPB, the stronger the behavioural intention, the more likely it will convert to actual behaviour. In view of the researcher's view of information security assessment as a behavioural issue it was deemed appropriate to base this study on the TPB. Figure 6.3 illustrates how attitude, subjective norms and perceived behavioural control determine intention and how this intention eventually becomes a behaviour.

Attitude toward the behaviour may be defined as the individual's positive or negative feelings about performing a behaviour (Azjen, 1991).

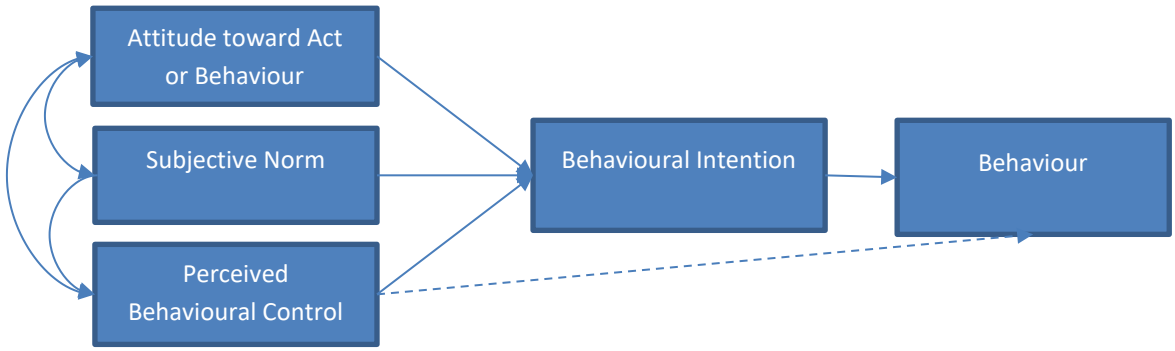


Figure 6.3: Theory of Planned Behaviour (Ajzen, 1991)

It is determined through an assessment of the individual's beliefs regarding the consequences arising from a behaviour and an evaluation of the desirability of these consequences. Attitude may be assessed as the sum of the individual consequence and desirability assessments for all expected consequences of the behaviour.

Subjective norm is defined as an individual's perception of whether people who are important to the individual think that the behaviour should be performed (Azjen, 1991). The contribution of the opinion of any given referent is weighted by the motivation that the individual must comply with the wishes of that referent. Hence, overall subjective norm may be expressed as the sum of the individual perception and motivation assessments for all relevant referents. This study was conducted in a traditional setting in which management was regarded as superior and, hence, as role models. Inherent in this set-up is the tendency to mimic each other's (subjective norms) behaviours. This implies that, in some instances, the employees' behaviour is merely enactment of management's behaviour.

Behavioural control is defined as an individual's perception of the difficulty involved in performing a behaviour. TPB views the control that people have over their behaviour as lying on a continuum from those behaviours that are easily performed to those requiring considerable effort and resources (Azjen, 1991).

Although Ajzen has suggested that the link between behaviour and behavioural control, as outlined in the model, should be between behaviour and actual

behavioural control rather than perceived behavioural control, the difficulty of assessing actual control has led to the use of perceived control as a proxy.

6.2.2. Knowledge Attitude Behaviour (KAB) Theory

The Knowledge Attitude Behaviour (KAB) Theory was developed by Kruger and Kearney (2006). The theory evolved from both behavioural intention and cognitive processing theories. Its main goal is to facilitate the factors that lead to behaviour. They cited three factors, all of which would affect employee compliance with information security initiatives. These factors/dimensions are knowledge (what they know), attitude (what they think) and behaviour (what they do). Each one of these dimensions may then be subdivided into focus areas on which the training and awareness programmes should be based. Where appropriate, and with the consensus of an organisation's management, these focus areas could then be further subdivided into specific subcategories. For example, the focus area of passwords could be broken down into two subcategories, namely, purpose of passwords and confidentiality of passwords. Confidentiality of passwords may then be further broken down into the writing down of passwords and the giving of passwords to others. In order to assist in the structuring process of a hierarchy of criteria Kruger and Kearney (2006) use a tree diagram as shown in Figure 6.4.

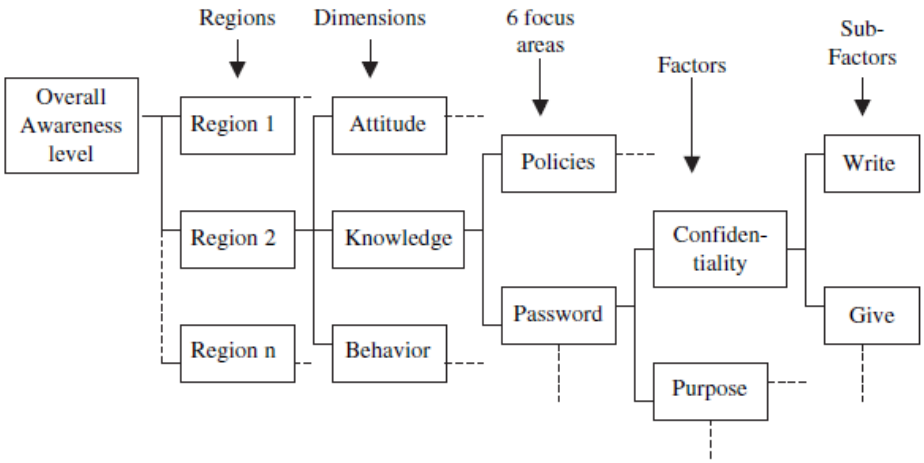


Figure 6.4: Tree Structure of Problem (Kruger & Kearney, 2006)

KAB was considered to be an influential explanatory theory for predicting employees' intentions to behave in a secure way (Da Veiga & Eloff, 2010; Parsons et al., 2010).

Information security awareness and training instils knowledge in employees and also assists in creating attitudes which, when combined, help employees to formulate their behavioural intentions (Kruger & Kearney, 2005). However, this theory lacks a practical relationship between actual behaviour and behavioural intentions and it relies on an assumption that intentions will convert into actual behaviour.

The KAB model has been criticised by some researchers. Bettinghaus (1986) identified a small, positive relationship between knowledge, attitude and behaviour while Baranowski, Cullen, Nicklas, Thompson, and Baranowski (2003) found weak evidence of its applicability within the health field. However, Helgeson, Van der Linden & Chabay (2012) examined its validity with regard to climate change and identified significant relationships between knowledge, attitude and behaviour. McGuire (1969) suggested that problems are not usually with the model itself but with the way in which it is applied. It is important to clearly conceptualise the type of knowledge that a particular study is examining. It is also essential to consider how the model relates to other variables of interest, and how these variables are measured (McCormac et al., 2017)

6.2.2.1. Knowledge

Based on the KAB model it may be postulated that employees' knowledge of information security related concepts, terms, threats, risks and possible countermeasures will influence their information security behaviour. For example, an employee who does not know what antivirus software is will not scan his/her computer and devices on a regular basis. In other words, limited knowledge will, in all likelihood, result in an employee demonstrating unsafe information security behaviour. However, obtaining such knowledge poses a challenge in the case of employees in SMEs as it is not possible to access some of this information easily. Nevertheless, the information security policies should incorporate this type of knowledge while awareness campaigns would help to disseminate it.

6.2.2.2. Attitude

The employees' awareness of information security is also influenced by what they 'feel' about information security. In other words, their individual perceptions of protecting information affect their actions. Understanding the importance of protecting this information and the negative consequences that may result if this information is compromised would affect their attitude. Thus, it may be said that attitude is inadvertently linked to what the employees know. However, this study did not not investigate influences which shape such attitudes when gauging the levels of information security compliance in the organisation in question.

6.2.2.3. Behavioural Intention

According to Kruger and Kearney (2006), employee information security behavioural intention should also be considered when information security compliance is assessed. Although actual behaviour is observed, the behavioural intent is based on the questions relating to participant behaviour and posed in the questionnaire. The inaccuracies and inherent challenges involved in using a survey to collect data may be exacerbated by the fact that the participants' recollection of their actual behaviour may be influenced by a desire to 'impress' the researcher and this may lead to a distorted account of the employees' actual information security behavioural intention. As a factor which is used in determining employee information security compliance behavioural intention may be referred to as perceived behavioural intent as it is based on a subjective account of the users' perceptions about how they have behaved/would behave

6.2.3. Deterrence Theory (DT)

Deterrence Theory (DT) predicts that an increase in the severity of the punishment imposed on those who violate the rules of the organisation reduces the incidence of certain criminal acts (Cheng, Li, Zhai & Smyth, 2014). The objective of DT is to increase prevention and deterrence in order to reduce unpunished abuse (D'arcy & Herath, 2011; Hu, Xu, Dinev & Ling, 2011).

DT is based on the premise that it is better to prevent than to punish. Deterrence involves the threat of punishment by means of some form of sanction and, thus, deterrence is, in fact, a way of attaining control through fear. Deterrence, in general, refers to the control of behaviour that is effected because the potential offender does not consider the behaviour worth risking for fear of the consequences of such behaviour (Kajzer et al., 2014). The essential elements of deterrence are certainty of punishment, severity of punishment and swiftness/severity of punishment (Cheng, Li, Zhai & Smyth 2014; Herath & Rao, 2009).

The deterrence may be either general or specific. The general deterrent effect of a sanction is the deterrent effect that a sanction has on a potential offender who has not personally had the sanction inflicted on him/her before, that is, the essence is the threat and not the experience of the sanction (Elliot, 2008). The special (specific) deterrent effect of a sanction is the deterrent effect which a sanction has on a special offender who has personally had the sanction inflicted on him/her before, that is, the offender has actually experienced the sanction (Elliot, 2008).

The literature clearly demonstrates that DT has been used extensively in the information security field to ensure that employees comply with information security requirements (D'Arcy & Herath, 2011; Cheng, Li, Zhai & Smyth, 2014; Kankanhalli et al., 2003). Blumstein (1978) states that if they are to be effective, the deterrence measures should put in place disciplinary actions that will be exercised when perpetrators are identified.

Cheng, Li, Zhai & Smyth (2014) proposed a theoretical model that integrates general Deterrence Theory and social norms theory. They argued that deterrence measures are indispensable for reducing employees' omission behaviours. Information security omission occurs when employees, who are aware of the organisation's security threats and countermeasures, fail to follow such countermeasures. Workman et al. (2008) term this phenomenon the knowing-doing gap. In addition, they believe that

social norms, such as subjective norms, play a critical role in understanding the omission behaviour of employees. A subjective norm refers to an individual's perception of "what those who are important think he/she should do in a given situation" (Bobek, Hageman, & Kelliher, 2013). DT focuses on sanctions as a measure for enforcing compliance with information security policies.

The literature highlights the importance of deterrent measures in reducing inappropriate behaviours on the part of employees (Kankanhalli et al., 2003; Pahnila, Siponen & Mahmood, 2007). Bulgurcu et al. (2010) argue that sanctions are believed to result in employees perceiving that there is a cost associated with not adhering to security-related rules and regulation. The studies conducted by Pahnila et al. (2007) and Herath and Rao (2009) found that factors rooted in DT significantly influenced the security compliance behaviour of employees. This study argues that deterrence measures reduce the risk of employees intentionally violating the organisation's information security policies.

Proponents of deterrence believe that knowledgeable employees choose either to obey or to violate policies after calculating the gains and consequences of their actions. However naïve employees may simply violate them due lack of knowledge. Overally, it is difficult to prove the effectiveness of deterrence since only those offenders who are not deterred come to the notice of policy enforcement and, thus, it is not actually possible to know why others do not offend. The initial DT doctrine was formulated by Beccaria (1963), who believed that 'employees want to achieve pleasure and avoid pain. Bad behaviour provides some pleasure, thus to deter bad behaviour one must administer some pain' (Bulgurcu et al., 2010). It is interesting to note that DT has become the dominant paradigm underpinning behavioural control in road safety around the world (Bates, Soole, & Watson, 2012).

6.3. Information Security Policy Compliance Reinforcement and Assessment Framework

Information security frameworks and models are proposed by researchers as a guide to organisations and to provide a structured approach to addressing issues relating to information security. This chapter discusses the development of an Information Security Policy Compliance Reinforcement and Assessment Framework. This framework was developed by combining and restructuring components of existing information security and behavioural theories. These theories were selected based on their potential applicability or relevance to employee behaviour in respect of information security. The framework was used to address the main research question as it may be used in determining the extent to which employee information security compliance may be influenced by awareness (knowledge), behaviours, behavioural intent and actual behaviours.

The proposed framework is based on the three existing theories which were discussed in Section 6.2, namely, TPB, KAB and DT. It is essential that any information security intervention should aim at increasing employees' security knowledge and encouraging compliance with information security policies. Findings from Parson et al.'s (2014) research on 500 Australian employees show that knowledge of the organisation's policy had a strong impact on attitudes towards policy compliance. The compliance mindset may be premeditated, as suggested by the TPB. The concept of reinforcement to eradicate omissive behaviour may be addressed by the Deterrence Theory of motivation which uses mandates and threats of punishment to motivate employees to behave in a secure way (Herath & Rao, 2009; Padayachee, 2012). The KAB theory of Kruger and Kearny (2006) assists in deciding what to measure and how to measure it when assessing compliance.

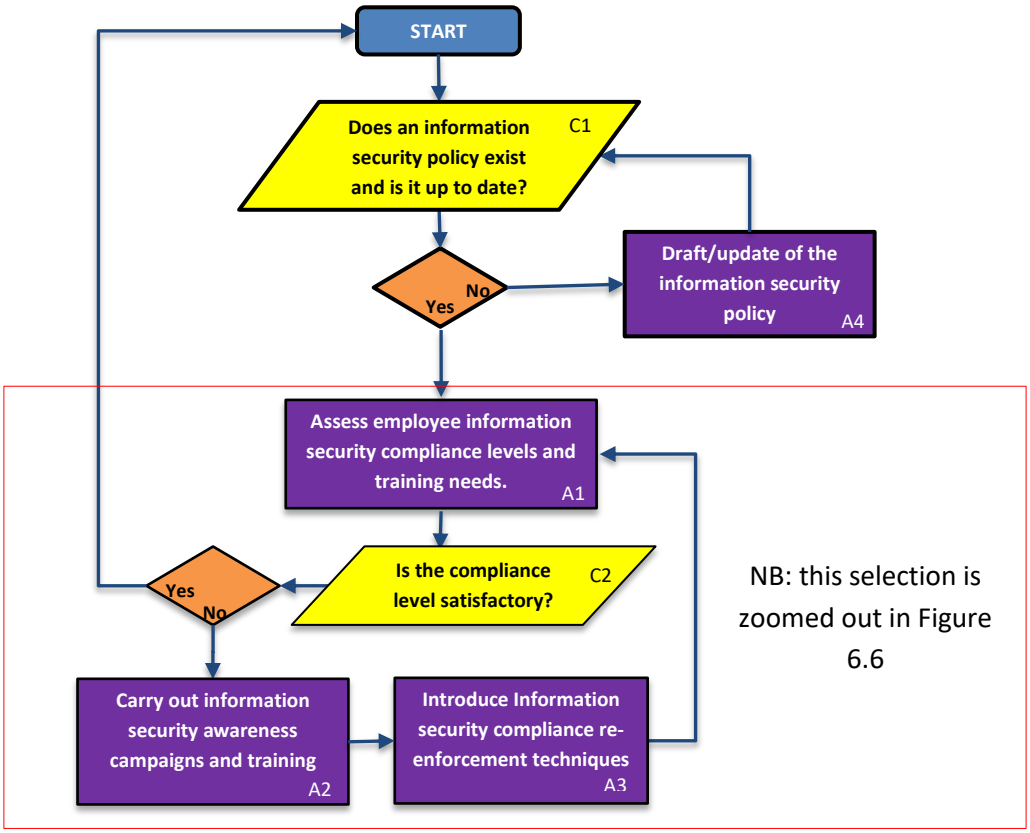


Figure 6.5: Information Security Policy Compliance Reinforcement and Assessment Framework

The framework proposed in this study is presented in Figure 6.5. The initial step as suggested in the framework involves checking for the existence of an information security policy (ISP); and then verifying whether it is up to date. However, during the empirical exploration conducted in this case study this was not carried out as the organisation had in place a sound and up to date policy that accurately reflected its overall stance towards information security. Hence, the process of drafting/updating an information security policy (ISP) was beyond the scope of the research. Figure 6.6 highlights the activities (A1, A2 and A3) detailed in the framework that are discussed next.

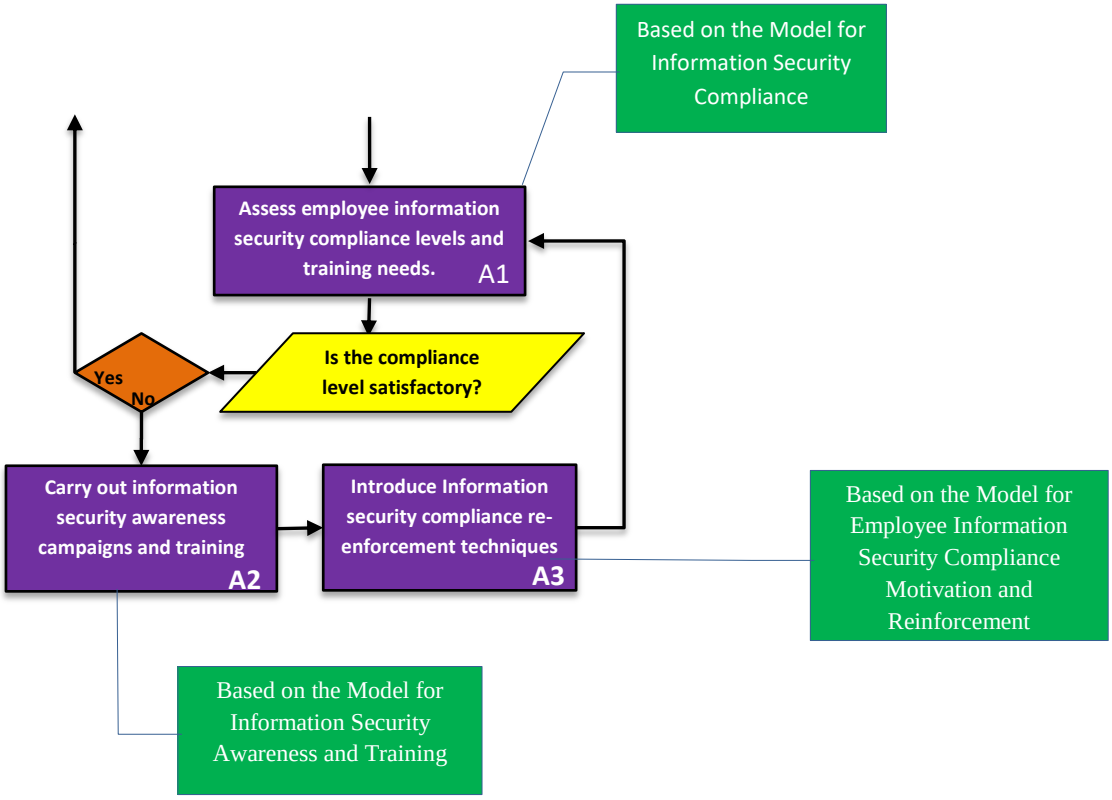


Figure 6.6: Section of the Information Security Policy Compliance Reinforcement and Assessment Framework

The framework included three models that supported the activities A1 to A3. The discussion of these models follows in Section 6.3.1 to 6.3.3

6.3.1. Model for Information Security Compliance Assessment

Information security theories posit that, if security efforts are to be effective, then it is incumbent on organisations to ensure that employees play a role in the security efforts (Da Veiga & Eloff, 2010; Russell, 2002; Schneier, 2008; Van Nierkerk & Von Solms, 2010). It is, therefore, reasonable to assert it is not possible to improve information security compliance unless it is possible to assess the employee compliance. No one would start a diet or exercise plan without having the means with which to measure its successes (or failures). Several managers have observed that "what gets assessed gets done" (ENISA, 2007). In addition, information security budgets are not unlimited and, hence, there is an increasing need to justify the expense of the controls which are implemented. Accordingly, either retaining or increasing information security resources often requires that the expected benefits be quantified and, thus, the importance of the information security compliance assessment.

Information for the baseline was gathered from surveys, observations, audits, specific security tests and help desk reports. After the security awareness campaign had been launched, it was important to measure the success of the campaign and to draw conclusions from the results. Measurement provides evidence of the campaign's effectiveness and reveals where knowledge gaps still exist. The measurements in this study were not limited to a verification of whether the message had been received by the target audience but also to ascertain the effectiveness of the message, method and behavioural intention change.

A survey conducted by Richardson (2008) found that 32% of the respondents in the survey did not measure information awareness in their organisations. The main reason for this was that there are no commonly agreed upon and understood standard measurements of the effectiveness of information security awareness and training. Two distinctive challenges may be identified when developing a measuring tool and doing the actual measurements, namely, what to measure and how to measure it? (Hinson, 2006; Kruger & Kearney, 2006).

Due to the lack of universally accepted measures of information security compliance training impact (Kruger & Kearney, 2005), a number of different qualitative and quantitative awareness measures have been used but there is little consensus on their effectiveness. This is clearly an area where good practice is evolving and emerging. However, assessing actual compliance, after a security intervention, is an essential component when considering the effectiveness of the intervention.

The proposed information security compliance assessment model aims to guide professional judgement with regard to employee information security compliance. In addition, it may also be used to assess information security awareness/training and compliance initiatives and to verify their efficacy by assessing the outcomes.

Organisations that do not measure information security compliance may be vulnerable to the following preventable errors:

a) Continuing an ineffective awareness and training programme with no real improvement in behavioural security.

b) Discontinuing an effective awareness and training intervention based on the incorrect subjective evaluation, perhaps because the intervention was erroneously perceived to be delivering no value.

As shown in Figure 6.7 the proposed framework encompasses a novel Model for Information Security Compliance Assessment. The constructs of this model were identified from the patterns revealed by the extensive literature review. According to TPB the intent to carry out a behaviour is dependent on both attitude and beliefs. Kruger and Kearney (2006) maintain that these beliefs and attitude are affected by knowledge. Hence, the proposed model is based on concepts in both the TPB and the KAB theories. The model comprises three main sections.

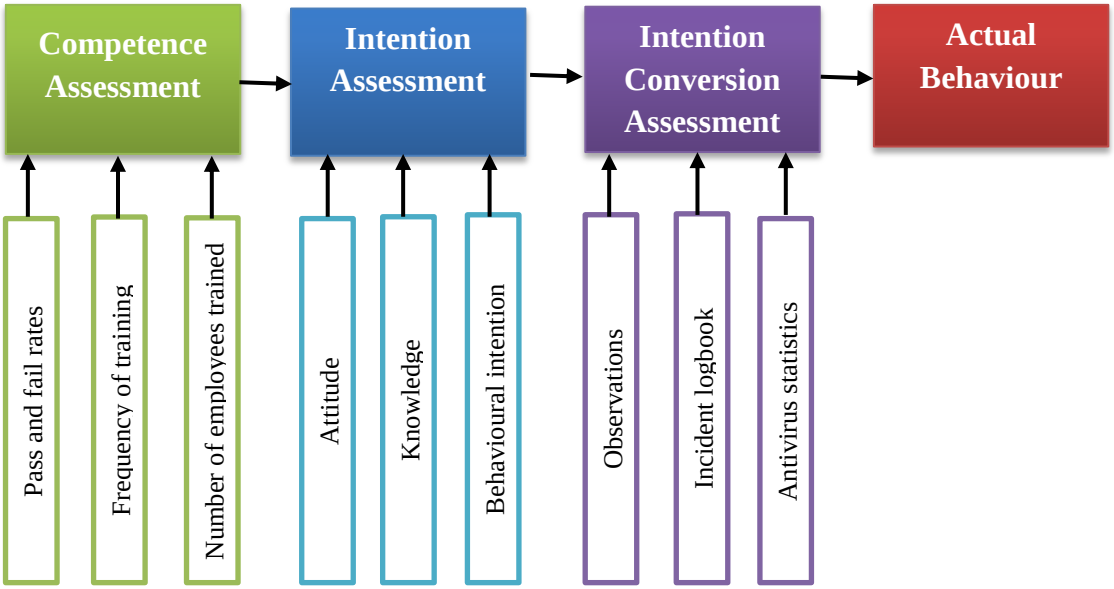


Figure 6.7: Model for Information Security Compliance Assessment

The competence assessment is related to the competence aspects of information security assessment, such as the number of employees trained, frequency of training and pass rates while the intention assessment addresses the intention assessment aspects such as knowledge, behaviour and attitude. On the other hand, intention conversion assessment focuses on aspects such as antivirus statistics, incident logs

and observations. The aspects measured by the information security compliance assessment model deliver insights into the effectiveness of security interventions.

6.3.1.1. Competence Assessment

It is recommended that the assessment of information security compliance includes operational measures. E-learning is one of the most efficient tools used in competence reporting. The learning management system that is used to administer the e-learning awareness programme provides numerous reports including those on completion rates and assessment scores. Demographic profiling by department, geography or other specific criteria is also possible. This level of assessment is particularly useful either for regulatory compliance or for internal or external auditing.

While the assessment of this type of quantitative data collected over a given period is a useful starting point as it provides an indication of trends in the levels of information security competence, it is not necessarily an indication of the effectiveness of either the training or of the compliance levels, which are affected by numerous different internal and external factors. When collected year by year, this data provides useful information showing the emergent gains of awareness/compliance initiatives. However, in order to gain a more comprehensive insight into the status of an organisation's information security, it is essential that such data is combined with intention and intention conversion assessments.

6.3.1.2. Intention Assessment

Once the basic routine and accurate reporting of competence assessment have been established, more in-depth assessments, such as intention assessment, become necessary. These measures focus on whether the observed trends in information security are directly related to information security compliance, and whether the training is having the desired effect in terms of both employees' *intended* security behaviour and the organisation's security culture.

When deciding on which intention attributes to capture, it is important to consider the key determinants of security behaviour from an employee perspective. Arguably, the

overall security stance of the organisation is enhanced when the attitudes, knowledge and behaviours of its employees are aligned with its security objectives and requirements (Kruger et al., 2006). Employees' attitudes towards information security are crucial because, unless they believe that information security is important, they are unlikely to work in a secure way, irrespective of how much they know about security requirements (Kruger & Kearney, 2005). Thus, attitudes may act as an indicator of an employee's disposition to act.

6.3.1.3. Intention Conversion Assessment

Prior to assessing intention attributes, both the problem behaviour (also known as the target behaviour) and the desired behaviour (also known as the replacement behaviour) should be clearly defined (Van Nes, 2010), that is, they must be stated precisely in observable and assessable terms. When a behaviour is described in observable terms, it may easily be discerned and documented. When it is stated in assessable terms, the behaviour may be quantified in some way (e.g. counted, calculated).

It is important to note that a variety of behaviours may serve the same function and, therefore, the intention definition should be sufficiently flexible to accommodate such variety (Van Nes, 2010). For example, if someone wants to transmit a file securely, he/she may use email encryption or write it to an encrypted USB stick and post it, or they may use a secure web-based mechanism to share the file.

6.3.2. Model for Employee Information Security Compliance Motivation and Reinforcement

Employees often unknowingly engage in risky behaviours that may threaten the security, privacy and integrity of organisational sensitive information or weaken the existing technological security perimeters (Al Hogail, 2015). Employees are responsible for a significant number of the security breaches organisations experience while a tiny security instance caused by employee error may be costly to

the organisation in terms of productivity lost while the restoration of the information systems is in progress, direct or indirect monetary value lost and/or the loss of the good will of the organisation's clients/customers (Steele & Wargo, 2007). This risky employee behaviour may be either intentional (malicious) or unintentional (naïve mistakes). However, either case may cause serious damage to the organisation's reputation and finances, and may potentially even harm the organisation's customers.

Thus, an organisation's information security effectively depends on the protective actions of its employees (Eminagaoglu et al., 2009; Ifinedo, 2014; Wilson & Hash, 2003; Peltier, 2005). Their compliance and good security practice, as detailed in the information security policies, is the best way in which to reduce the probability of information security breaches. Such "good practice" refers to the set of core information security activities that must be applied by employees in order to ensure that information security is maintained.

Information security awareness efforts are designed either to change behaviour or to reinforce good security practices and enforce compliance (Eminağaoğlu et al., 2010; Ifinedo, 2014; Wilson & Hash, 2003). Effective information security awareness programmes may, ultimately, improve the organisation's efficiency as these programmes will allow the organisation to focus on techniques that will improve their employees' security behaviour in the interests of a more efficient organisation (Stephanou & Dagada, 2006).

In line with the objectives of this study, a structured information security compliance/reinforcement which seeks to reduce the employee knowing-doing gap was also developed and examined. This model (shown in Figure 6.3) builds on the Deterrence Theory and specifically, targets employees' intentional disregard of the information security policies and procedures for reasons other than malicious purposes but, rather, reasons such as convenience, disregard for the rules, or lack of understanding. This model may also be prescriptive by focusing security awareness

training efforts on influential areas and serving as a metric for assessing changes in user attitudes towards observing and following information security policies and procedures.

The Model for Employee Information Security Compliance Motivation and Reinforcement, which is presented in Figure 6.3, is based on the theoretical framework discussed in section 6.2. It may be said that the TPB, DT and KAB theory may be used to explain how behaviours may be manipulated to be desirable behaviours. The model presented in Figure 6.8 fuses the theories together to construct a model that may be adapted by engineering SMEs so as to enable them to achieve information security compliance.

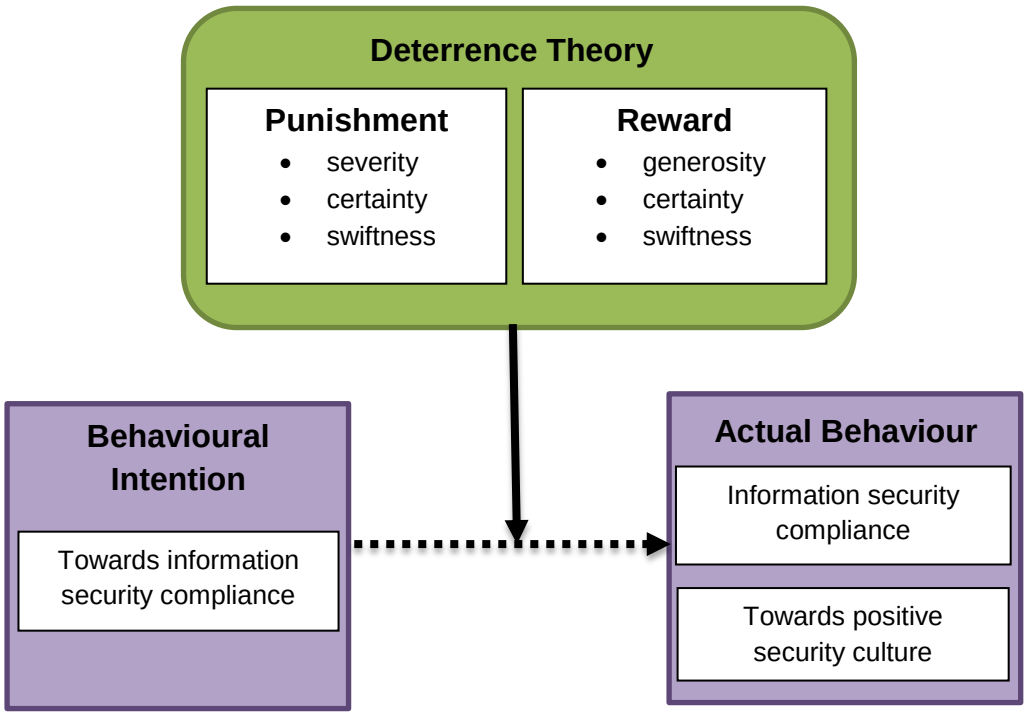


Figure 6.8: Model for Employee Information Security Compliance Motivation and Reinforcement

The model relies on punishment or rewards to enforce compliance. These punishments and rewards are based on three individual components, namely, severity or generosity, certainty, and celerity. It is thought that the more severe a punishment or the more the generous the reward, the more likely it is that a rationally calculating employee will comply. Certainty simply means making sure that punishment takes place whenever there is non-compliance and a reward given

whenever there is compliance. Classical theorists such as Beccaria (1963) believe that, if employees know that their undesirable acts will be punished, they will refrain from offending in the future. In addition, the punishment or reward must be **swift** in order to motivate compliance. The closer the application of the punishment or reward is to the commission of the act, the greater the likelihood that employees will be motivated to convert intentions into actions.

In short, deterrence theorists believe that, if punishment is severe, certain, and swift, a rational person will measure the gains and losses before engaging in risky behaviours and will be deterred from non-compliance if the loss is greater than the gain.

However, there is literature that shows conflicting results for the effectiveness of the sanctions employed to overcome the problem of employees' negligent information security compliance (Herath & Rao, 2009; Kankanhalli et al., 2003). In other words, deviating from the premise of the Deterrence Theory, employees' violation of information security policies is not always best addressed by the fear of sanctions because employees often rationalise to minimise the perceived harm of their policy violations (Siponen & Vance, 2010). On the other hand, this theory is being used successfully worldwide for traffic law enforcement.

6.3.3. Model for Information Security Awareness and Training

Information security campaigns are divided into awareness and training. Awareness aims to raise the collective knowledge of information security and its controls, while training aims at facilitating a more in-depth level of employee information security understanding. Both training and campaigns aim at persisting attitudinal and behavioural improvements on the part of employees towards compliance with information security policies and instructions. These approaches utilise persuasive communication. An effective information security awareness and training programme seeks to explain the proper rules of behaviour when using the organisation's ICT resources. Thus, the programme communicates the information security policies and

procedures that need to be followed. Awareness and training must precede and sanctions must be imposed when noncompliance occurs (Herath & Rao, 2009). Figure 6.9 depicts the proposed Model for Information Security Awareness and Training.

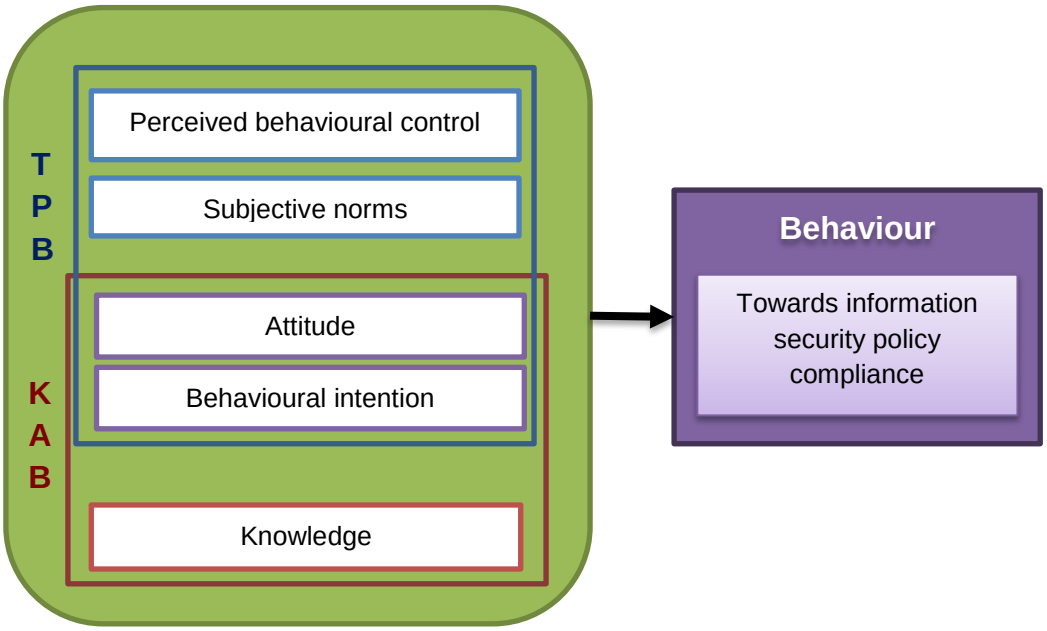


Figure 6.9: Model for Information Security Awareness and Training

This proposed model combines the Knowledge, Attitude and Behaviour Theory with the TPB. These theories have two constructs in common, namely, attitude and behavioural intention.

The proposed model suggests that awareness campaigns should aim at the following:

- **Perceived behavioural control** – Change the employee perception of behavioural control. The usually underestimate their capabilities.
- **Subjective norms** – Communicating the position of the management towards security.

- **Attitude** – Change employees attitude towards security from thinking it interferes with their daily routines to, it helps with their daily routines.
- **Behavioural Intention** – It should motivate employees to want to behave securely.
- **Knowledge** – It should assist in educating employees and keeping them updated regarding risks and secure behaviours.

If the above are combined this should change employee behaviour towards policy compliance.

The BERR (2008) survey suggests that the majority of organisations rely upon written materials of some form. However, merely developing and circulating a policy are not be sufficient to foster the appropriate understanding and behaviour. The majority of companies use the traditional classroom style for awareness and training. However, this study sought to apply the now widely used e-learning concept to information security awareness and training (refer to CD in Appendix B). Jenkins, Goal, and Morrele (2008) and Ricer, Filak, and Short (2005) reported that there is no significant difference between people who learn using a computer or the traditional classroom style in either the short or long-term retention of knowledge.

6.4. Conclusion

The human factor is often underrated or underplayed in the securing of information assets. It is crucial to ensure that employees act and behave securely. As this study has shown merely providing employees with knowledge and know-how does not achieve this. Thus, although such knowledge and know-how are essential, they are not sufficient to ensure compliance. Assessing actual compliance is crucial if the areas of non-compliance are to be exposed in order to identify those areas that require more focused attention. Moreover, such compliance assessment provides evidence of the competence-driven value which may be used to justify the resources used in such information security endeavours.

Although several organisations are struggling to quantify security compliance it is essential that it is assessed in order to verify whether or not their security initiatives are taking effect. This chapter discussed the challenges involved in using the behavioural intention-based information security assessment tools. The chapter also discussed the gap between knowing and doing and then proposed an Information Security Policy Compliance Reinforcement and Assessment Framework in an to attempt to combat these issues. The next chapter discusses the empirical exploration undertaken in the study and during which the model was validated and refined through action research.

CHAPTER 7 - RESEARCH METHODOLOGY

Chapter 7:

This chapter provides an overview of the methodological stance adopted in the study. This methodological stance is discussed in terms of the research paradigm, ontology, and epistemology. The theoretical philosophies which influenced the methodological approach adopted are discussed in detail in the chapter. Finally, the chapter explores the evaluation of the research and ethical considerations.

7.1. Introduction

Mouton's (1996) view of research is the application of a variety of standardised methods and techniques in the search of valid knowledge. Research is viewed as scientific therefore it is essential to conduct it systematically, sceptically and ethically (Robson, 2002). The philosophical paradigm acts as a guide for the researcher by outlining the philosophical underpinnings of the research as well as the underlying assumptions or intellectual structure upon which the research is based (Denzin & Lincoln, 2011). Researchers make assumptions about both the nature of reality (ontology) and also about the way in which knowledge is constructed (epistemology). While the paradigm provides an insight into the researcher's assumptions about the nature of reality and the construction of knowledge, the methodological dimension addresses the following questions (Mouton, 1996), namely, "How do we attain knowledge?" and "How do we ensure we reach our research goal?"

The scientific quest for knowledge follows a structured approach in terms of which theory informs the research questions which, in turn, influence the research design and research methods selected. In addressing the research questions the methods selected determine the type of data that will be collected and analysed. This research is a social science study of human behaviour. Comparing the natural and the social sciences, Punch (2013) suggests that, natural science builds explanatory theory to justify its data, while social science builds an explanatory theory about human behaviour which is based on and tested against real-world data.

In any research project the researcher seeks to discover new knowledge or facts in a systematic or organised manner in order contribute to the existing body of knowledge (Saunders et al., 2009). For this study, this task started with the careful selection of an area of interest, research topic, and a research paradigm. Wilson (2008) maintains that understanding the research paradigm enables a researcher to decide on the overall research strategy to be used in a particular research project by

suggesting the most appropriate way in which to gather and interpret the evidence required to answer the research question.

This chapter (see Figure 7.1 below) discusses the philosophical assumptions, research design and research methods which formed the basis of the data collection and data analysis processes in this study. Research implies a progression from underlying philosophies, assumptions and theory to actual knowledge. The research approach adopted in attempting to understand human behaviour is different from the causal approach adopted in studying the natural sciences.

In considering the most widely discussed philosophies, interpretivist was deemed to be the most suitable paradigm for achieving the goals of this study. The research paradigm influences the design and methodologies used in a study, including the strategies and research instruments, as well as the data collection and data analysis methods.

Action research was identified as the most suitable design for the purposes of this explanatory research study. While taking into account a research study's objectives, a research endeavour may be broadly classified as descriptive, correlational, explanatory or exploratory. Descriptive research attempts to systematically describe a situation, phenomenon or problem while attempting to clarify why and how there are relationships between various aspects of such situations, phenomena or problems calls for explanatory research (Kumar, 2005). Correlational research focuses on the discovery or establishment of the existence of a relationship/association/interdependence between aspects of a situation while exploratory research is undertaken when either exploring an area about which little is known or investigating the possibilities of undertaking a certain research study (Kumar, 2005).

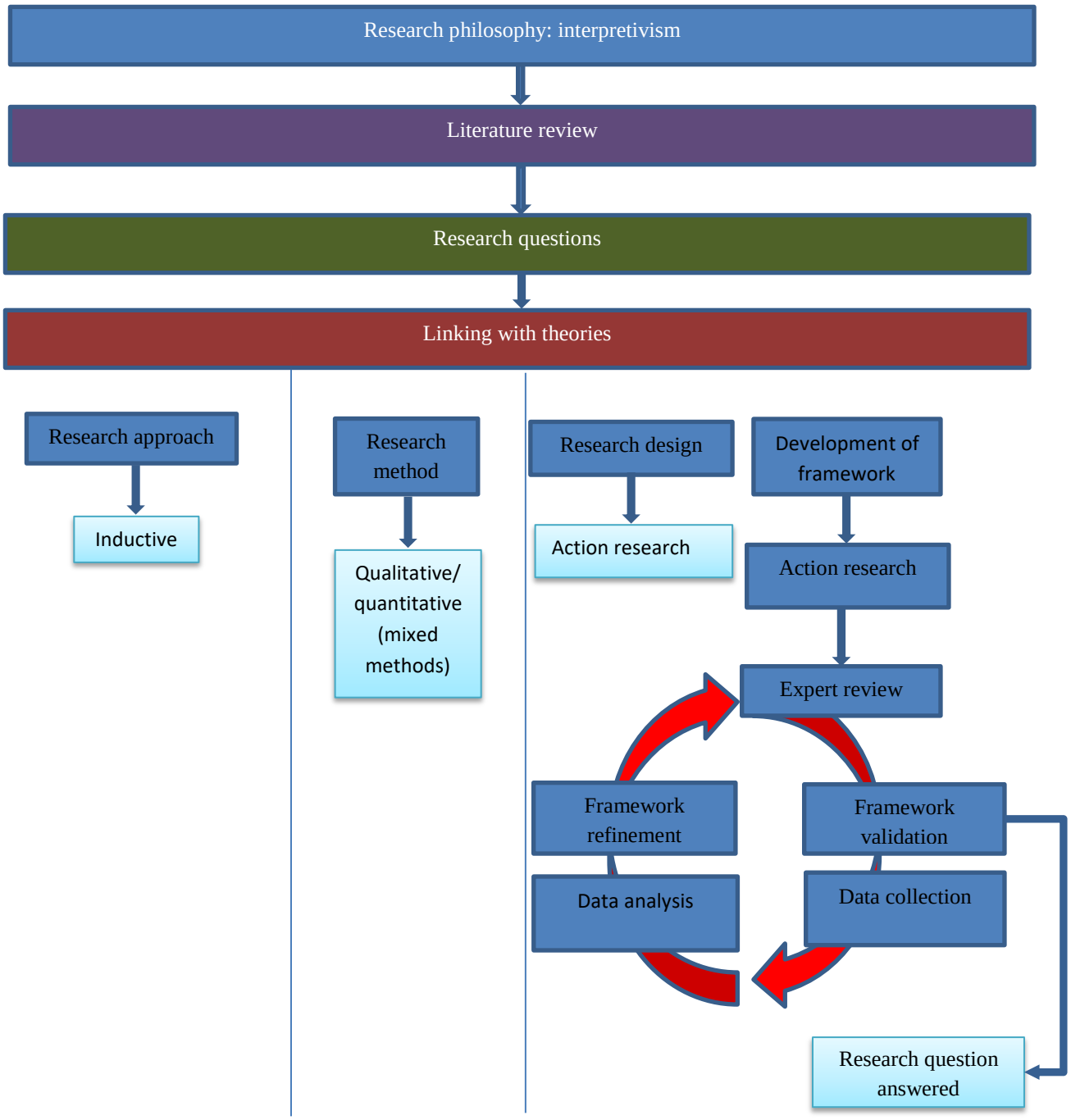


Figure 7.1: Research Design Diagrammatic Overview

In the pursuit of scientific knowledge the main objective is explanation and not just description, thus creating an inextricable link between theory and explanation (Punch, 2005). Action research makes provision for the inductive approach to research in terms of which knowledge is unearthed or evolves. The methods and techniques applied in this study's pursuit of valid knowledge are also outlined in this chapter. Surveys, document analysis and participant observation were used as the

main data collection methods in the study. Questionnaires, observations, log checks were used to evaluate the participants' levels of information security awareness during different stages of the action research iterations.

The study grouped the interpretivist paradigm inquiry tasks and activities into the following three categories, namely, design strategies (research paradigm and research design), data collection (research methods) and analysis strategies (data analysis). The research approach is discussed in the next section. Patton (1987) supports the formulation of an approach, highlighting the appropriateness of the provision of a framework for assisting with decision making and action by linking supposedly isolated tasks and actions and incorporating efforts with a common purpose.

7.2. Research Paradigm

This study adopted the framework proposed by Terreblanche, Durrheim and Painter (2006) which views the research paradigm as describing the nature of enquiry within three dimensions, namely, ontology, epistemology and methodology (see Figure 7.2). Social science research approaches are usually compared along these dimensions with the ontological dimension relating to the existence of the real objective world; the epistemological dimension relating to the possibility of acquiring knowledge of this world and how this knowledge is formed and, lastly, the methodological dimension referring to the technical instruments used in the knowledge acquisition process (Della Porta & Keating, 2008).

Unlike theories which attempt to explain, paradigms do not explain anything but provide a logical framework which may be used in creating theories (Babbie, 2007). Kumar (2005) refers to two main paradigms which form the basis of social science research, namely, the positivist approach and the interpretivist approach.

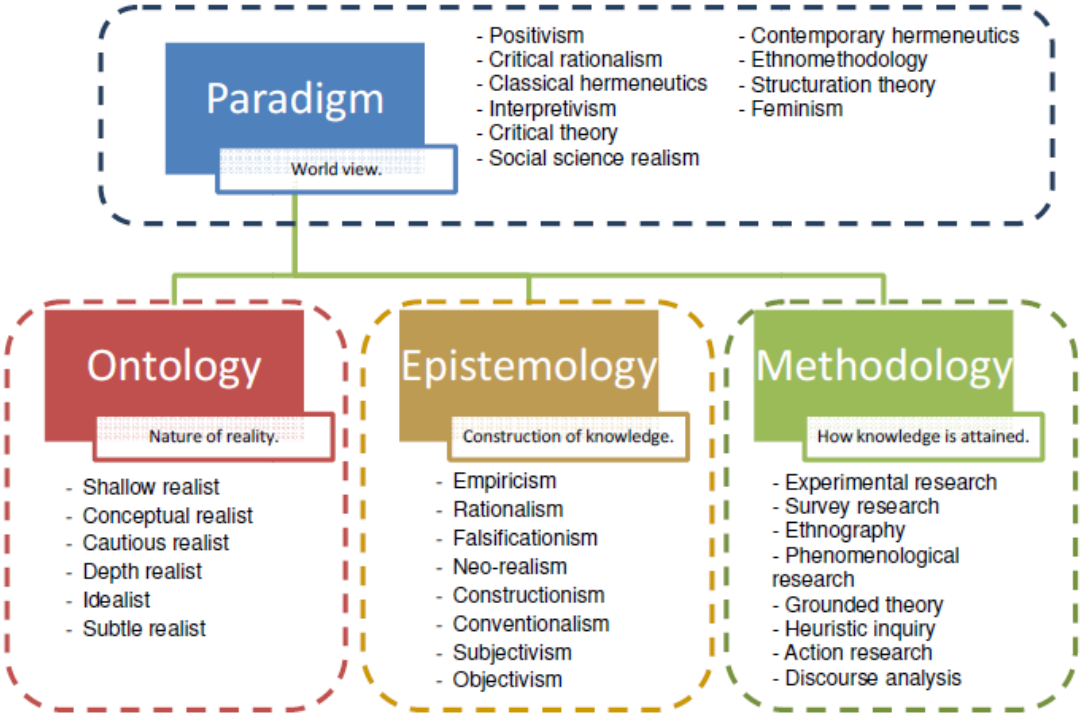


Figure 7.2: Research Paradigm Dimensions (Nqoqo, 2014)

Kumar (2005) advocates that researchers follow certain principles such as controlling bias and maintaining objectivity in both the research process and the drawing of conclusions. In its aim to understand the subjective knowledge of the employees this study adopted an interpretivist approach. Figure 7.2 shows ten research paradigms however the researcher felt only two would be ideal for this inquiry and are discussed in more detail in Sections 7.2.1 and 7.2.2 and section 7.2.3 discusses the rational of the final choice.

7.2.1. Positivism

Positivists are of the belief that reality is stable, observable and describable from an objective viewpoint (Alexander, 2014), i.e. without contact or interference with the subject matter being studied.

Previously observed, explained realities and their inter-relationships may be used for predictions. "Positivism has a long and rich historical tradition. It is so embedded in our society that knowledge claims not grounded in positivist thought are simply dismissed as not scientific and therefore invalid" (Alexander, 2014). Alavi and Carlson (1992) indirectly supported this view in their review of 902 information

systems research articles, which found that all the empirical studies were positivist in approach.

7.2.2. Interpretivism

Interpretivists contend that reality may be fully understood only through subjective interpretation. Hence, interpretive researchers are of the belief that reality consists of human being's subjective experiences of the external world. According to Potrac, Jones and Nelson (2014), interpretivists believe there are multiple routes/methods to knowledge and neither of them is 'correct' nor 'incorrect'.

Interpretivists derive their constructs from an in-depth examination of the subject matter. Gephart (1999) argues the assumption that knowledge and meaning are acts of interpretation and, hence, knowledge is subjective to human thinking and reasoning. This is why one of the keys to the interpretivism philosophy is acknowledging that scientists are not able to avoid affecting the subject matter of the study and admitting interpretation diversity. However, interpretivists maintain that these interpretations are part of the scientific knowledge being pursued.

Walsham (1995) presents the following three applications of theory in interpretive studies, namely, iterative process of data collection and analysis theory; design and data collection theory and the studies outcome as a theory. This research study made use of theory as an iterative process between data collection and data analysis.

7.2.3. Discussion and Rationale for Choice of Approach

It has often been observed that no single research paradigm is intrinsically superior to any other paradigm and many authors now prefer the use of a combination of paradigms in order to improve the quality of their research (Creswell, 2013; Johnson, Onwuegbuzie & Turner, 2007). This study acknowledges that all paradigms are valuable if used appropriately and that, if managed carefully and it is common for research to include elements of both the positivist and interpretivist approaches.

However, there has been much debate on whether or not the positivist paradigm is entirely suitable for the social sciences with many authors calling for a more diverse attitude towards information systems research methodologies (Urquhart & Fernandez, 2013; Myers, 1997; Dubé & Paré, 2003). Information systems deal with the interaction of humans and technology and, thus, they should be considered as a social science rather than a physical science (Pechmann, Zhao, Goldberg & Reibling, 2003). Some of the difficulties and apparent inconsistencies experienced in information system research may, therefore, be attributed to the positivist paradigm being inappropriate for this domain. In addition, some variables or fundamental aspects of reality that may have been previously deemed to be unmeasurable under the positivist paradigm were unresearched (Chou, 2007; McKelvey, 2009).

The fundamental concern is that the research paradigm chosen should be both relevant to the research question (set out in Chapter 1) and operationally rigorous. The interpretivist philosophy was used in this study because the study included an element of facilitating behavioural change. This is subjective and is also difficult to carry out without involvement with the subject matter.

Various elements of the research approach selected are further elaborated upon in the following sections: Research Approach, Research Methods, Research Design, and Framework Development.

7.3. Research Approach

This study adopted Blaikie's (2010) narrow definition of a research approach (logic of inquiry or strategy) which regards it as a starting point which provides a set of steps for answering research questions.

Saunders et al. (2009) posit that the research process includes two possible approaches, namely, induction and deduction. According to Ormston, Spencer, Barnard and Snape (2014), "induction is the formation of a generalisation derived

from the examination of a set of particulars, while deduction is the identification of an unknown particular, drawn from its resemblance to a set of known facts".

The deductive approach is the reverse of inductive reasoning. According to Evans, (2013), during deductive reasoning hypotheses are generated prior to the research process and then modified through a process of falsification, validation or verification by conducting empirical research. Table 6.1 presents a logical view of the research approaches discussed.

Table 7.1: Research Logical Views (Mason, 2002)

Strategy	View	Description
Deductive	"Theory comes first"	Hypotheses are generated in advance of the research process, and then modified – usually through a process of falsification – by the empirical research.
Inductive	"Theory comes last"	Theoretical explanations are developed out of the data in a process. This process is commonly seen as moving from the particular to the general.

The main difference between deductive and inductive research is their respective starting positions (see Figure 7.3 and Table 7.1). Deductive research starts with a theory and then seeks data that will either corroborate or falsify the theory in question while inductive research starts with data which is then used to formulate a theory in order to explain the data.

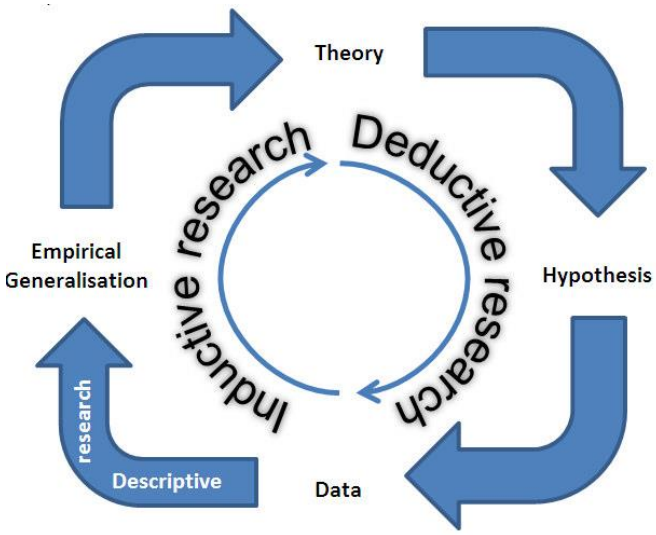


Figure 7.3: The Research Circle (Chambliss & Schutt, 2012)

Some researchers have agreed that these approaches are not mutually exclusive. For example, inductive reasoning may progress to deductive research if unexpected patterns are discovered in the data which has been collected (Chambliss & Schutt, 2012). The next section discusses the research method used in this study.

This research used inductive logic and began with an extensive literature review of existing information. In line with inductive research, the study started progressing by picking up general ideas, theories, patterns and in/consistencies within information security. Gaps in literature that stimulated Interest were and tentative perceptions were developed, explored and, finally, conclusions were formulated.

7.4. Research Method

According to Creswell (2013), a research method is “the plan or blueprint according to which data is to be collected to investigate the research hypotheses or question in the most economical manner”. On the other hand, Myers (2013) defines a research method as “a strategy of enquiry, which moves from the underlying assumptions to research design, and data collection”. An important decision to be made regarding the research methodology to be used in a study is whether the study will be primarily quantitative, qualitative or mixed. Myers (2013) also suggests that social and cultural phenomena should ideally be researched using qualitative methods. The fact that the natural human ability to communicate and the ability to provide insight into the social and cultural context are not effectively reflected in quantitative methods has increased the use of qualitative methods (Myers, 1997). However, combining both research methods is likely to result in more substantial findings and conclusions that are accurate than would have been the case if either qualitative or quantitative research only had been used (Johnson, Onwuegbuzie & Turner, 2007).

In order to understand the mixed method approach, it is important to first discuss the differences between the quantitative and qualitative approaches. The distinctions between qualitative and quantitative research lie in the data collection and data analysis procedures as well as the presentation of the results. Quantitative research

usually produces statistical results while qualitative research produces descriptive data in the form of narrations. Qualitative researchers study subject matter in its natural setting and attempt to make sense of phenomena in terms of human interpretation (Denzin & Lincoln, 2011). Table 7.2 presents the differences between qualitative and quantitative research as cited by Thomas (2010).

Table 7.2: Differences between the Quantitative and Qualitative Approaches (Thomas, 2010)

Orientation	Quantitative	Qualitative
Assumption about the world	A single reality, i.e., may be measured by an instrument.	Multiple realities
Research purpose	Establish relationships between the variables measured	Understand a social situation from the participants' perspectives
Research methods and processes	- Procedures are established before the study begins; - A hypothesis is formulated before research begins; - Deductive in nature.	- Flexible, changing strategies; - Design emerges as data is collected; - A hypothesis is not needed in order to begin the research; - Inductive in nature.
Researcher's role	The researcher is ideally an objective observer who neither participates in nor influences what is being studied.	The researcher participates and becomes immersed in the research/social setting.
Generalisability	Universal, context-free generalisations	Detailed, context-based generalisations

Recognising the lack of objectivity which is sometimes associated with interpretivist qualitative research methods, the quantitative approach was adapted to complement both the data collection and the data analysis carried out in this study, hence making this a mixed methods study. Although the mixed methods approach is less popular than either the qualitative or the quantitative approach, it, nevertheless, allows the use of methodological tools from either approaches as is deemed necessary to answer the research questions (Teddlie & Tashakkori, 2009). According to Johnson and Onwuegbuzie (2007), mixed methods research designs may be divided into two major types, namely, the mixed-model which combines the qualitative and the quantitative approaches within or across certain stages of the research process and the mixed method which includes both the quantitative approach and the qualitative

approach throughout the entire research study (Johnson & Onwuegbuzie, 2007). This study used the mixed-model which combined the qualitative and the quantitative approaches only during the data collection and the data analysis. This model is depicted in Figure 7.4.

Figure 7.4: Mixed Method Research Process Model

7.4.1. Sources of Data

Both primary and secondary data sources were used for the purposes of this study. Although these two data sources both have their advantages and disadvantages they do complement each other in different research scenarios. These data sources are explained further in sections 7.4.1.1 and 7.4.1.2.

7.4.1.1 Primary Data

Primary data refers to information collected by a researcher for a specific research endeavour. Primary data is usually collected in instances were nothing has been compiled and published, were nothing is in the public domain or available sources are unreliable. Researchers or sponsors generally spend time allocating the resources required to gather the primary data only when a question, issue or problem is sufficiently important or unique to warrant the resources used in gathering the primary data.

Advantages of Primary Data Use for This Study:

- Collection of original and relevant data.
- Current data that provides a realistic view of the subject matter.

- High reliability of data because it is collected by a concerned and reliable party for a specific purpose.

Disadvantages of Primary Data Use for This Study:

- It was time consuming
- Some did not answer the questionnaire/online test timeously.

The main instruments used to collect the data required in this study were questionnaires, expert review, interviews, log reports and observations. The next section provides details on the way in which the questionnaires were administered and additional information collected.

7.4.1.2. Secondary Data

Secondary data refers to data that was collected for some other purpose and at a different time in the past by a party not related to the research study in question. If a study makes use of such data then its regarded as secondary data in respect of the current users of such data. Secondary data may be found in any form (written, typed or electronic).

In order to gain an initial insight into the research problem the use of secondary data was necessary. Secondary data is classified in terms of its source, namely, either internal or external. Internal secondary data refers to secondary data that is acquired from within the organisation where the research is being carried out while external secondary data is obtained from outside sources. This study made use of both internal and external secondary data. The next section discusses the various advantages and disadvantages of using secondary data.

Advantages of Secondary Data Use for This Study:

- It was faster to access as compared to primary data.
- It allowed the use of work of the best scholars all over the world.
- Guided the path of the study.

- Saved time, effort and money.

Disadvantages of Secondary Data Use for This Study:

- The reliability of the data was unknown
- Data collected in other geographical locations may not be suitable for this study due to variable environmental factors

Having considered the advantages and disadvantages of primary and secondary data sources, the data requirements of this research study and the time factor, it was decided to use both sources of data in amalgamation to ensure proper coverage of the research topic. The primary data was collected from employees of the company, antivirus logs, incident report logs and employee behaviour observations while the secondary data was collected from journals, conference proceeding, books, newspapers, magazines, white papers and the internet. The primary and secondary data was collected in order to cover every aspect of the study. The primary data was related to the behaviour and responses of the employees while the secondary data referred to all related research that had been conducted previously.

7.4.2. Instruments for Primary Data Collection

Ellis and Levy (2012) categorise data in terms of two dimensions, namely, proximity and method, adding that these two dimensions are particularly useful in the context of scholarly research. They defined proximity as “the degree of separation between the actual phenomena of interest and the method in which it is observed and measured” and stated that method referred to “the degree to which the data can be objectively or subjectively represented”. These two dimensions are then subdivided into two levels: namely, for proximity direct and indirect measures and for method qualitative and quantitative data. Direct data arises from direct observations of the subject matter while indirect data is derived from indirect observations of representations of the phenomena but not from the subject matter itself (Ellis & Levy 2012). Table 7.3 provides an overview of research methods and associated data collection instruments. For the purposes of this study the data collection was made

more rigorous by combining instruments from both the qualitative and quantitative methods as this was a mixed methods study.

Table 7.3: Research Methods and Data Collection Instruments Used (adapted from Ellis & Levy, 2012)

		Research Method	
		Qualitative	Quantitative
Proximity of the Measure	Direct	• Historical non numerical records • Open-ended questionnaires • Interviews • Direct observations	• Historical numerical records • Surveys • Numerical simulations • Test results
	Indirect	• Open-ended questionnaires • Interviews • Observations	• Surveys • Numerical simulations • Test results

This study made use of the following direct qualitative tools, namely, historical non numerical records, open-ended questionnaires, interviews and direct observations, and the direct quantitative tool of historical numerical records. The data collected was analysed, compared and categorised and then triangulated and interpreted to enable the researcher to draw conclusions. The primary data instruments used to collect the data for this study are explained in detail in the sections that follow.

7.4.2.1. Questionnaire (Direct)

Questionnaires are a vital instrument for data collection properly constructed and responsibly administered, however, inappropriate questions, incorrect flow of questions, incorrect scaling or a weak questionnaire format may make the instrument inaccurate therefore valueless as it may not accurately reflect the participants views and opinions (Thomas, 2010). To minimise the chances of such, this study checked the questionnaire ensuring it accurately captured the required data by pre-testing them on individuals not part of the study. This checking served four basic purposes: namely, (1) ensuring it was collecting relevant data, (2) ensure the data could be comparable across the different iterations for analysis purposes, (3)

reducing bias, and (4) to ensure the questions would stimulate and engage the participants.

This study used three questionnaires as discussed below:

- **Interview questionnaires** on information security compliance and behavioural intent were administered to the participants. The aim of these questionnaires was to determine the respondents' attitude, knowledge and behavioural intent towards information security as well as their perceptions of and concerns about the approaches to safeguard the information asset in the workplace (Appendix C);
- **Expert evaluation questionnaire** (Appendix C).

The questionnaires were divided into two sections, namely, open-ended questions which focused on the respondents' level of security awareness as well as their security behavioural intent, and close-ended questions that offered a set of pre-designed replies such as "Yes/No", "True or False", multiple-choice responses and the choice of numbers representing strength of a feeling or attitude (5-point Likert). Open-ended questions tend to be unstructured, thus giving the respondents a feeling of freedom in their answers. The questionnaires requested all the participants to respond to the same questions which were organised in a predetermined order. Regenbrecht, Schubert, Botella and Baños (2017) considers the questionnaire to be ideal as a way of asking standardised questions while it also facilitates an analytical approach to exploring the relationships between variables. The questionnaires were individually completed by the respondents online. The participants were asked to respond to statements on security compliance concepts and security behaviour/perceptions, for example, "Do you keep sensitive, personal data (e.g. passwords, bank codes) on your work computer?" The online setup in which the questionnaire was administered to the participants is discussed in Chapter 8.

7.4.2.2. Observations (Direct)

According to Gray (2009), “observation involves systematically viewing people’s actions and recording, analysing and interpreting their behaviour”. The advantage this study benefited from observations was the ability to observe both group and individual behaviour. The disadvantage was the observer/researcher could not be watching everyone at the same time and hence might have missed some trends.

This study used structured observation which is more quantitative than qualitative in nature. For example, phishing emails, checking user workstations for passwords on post-it-notes, the nature of passwords, and computer locking when the user was not close to his/her workstation were used to observe the actual security behaviour of the participants/employees. This method was selected as the most suitable method of determining actual employee security behaviour related to the information security focal areas which were included in the main questionnaire which was used to collect the data required for the study. The observation of the actual security behaviour of the participants was designed to complement the data collected and, thus, enhance the credibility of the data. The observations were recorded for the pre-structured aspects observed. Care was taken to ensure the comments made were non-judgmental, concrete descriptions of what was observed.

7.4.2.3. Historical Numerical and Non Numerical Records (Direct)

Historical records comprise written sources, log evidence and, in some instances, oral sources. Within the framework of information security compliance, historical records may be defined as any type of evidence emanating from past activities. Different levels of authority may be assigned to such records. The historical method has established itself as the optimal working method in information security (e.g. study of antivirus logs).

7.4.2.4. Interviews (Direct)

According to Brinkmann (2014), the interview is a method of gathering information through verbal interaction. The interviewer non-judgmentally collects the data from the participants and cross examines it. It is vital that the interviewer is very strategic,

efficient and tactful if he/she is to obtain accurate and relevant data from the participants (Brinkmann, 2014). Combined with observation, interviews enable the researcher to understand the meanings that everyday activities hold for people.

This study made use of semi-structured informal interviews. These used both closed and open questions. For the sake of consistency with all the respondents the researcher prepared pre-planned, core questions for guidance. However, as the interviews advanced, the employees were given the opportunity to elaborate and provide more relevant information. The main benefits of using this instrument were:

- Direct contact with the employees often lead constructive suggestions
- Helped to collect data for some of the non-responded questionnaire questions by collecting the data personally.
- Only a few participants were required in order to gather rich data
- Allowed for cross examination of data.

7.4.3. Participants in the Study

The participants in this research study were thirty employees of a civil engineering SME in South Africa. These employees ranged from the very technically inclined to the least. This population comprised of all the employees of the company making high chances of proportional skill level distribution amoungst them.

7.5. Research Design

The researcher employed an action research design for this study on employee information security behaviours. Action research (AR) is an established research method which has been used in the social and medical sciences since the mid-twentieth century. AR is particularly valuable in view of its ability to inform theory while making a practical difference. AR was originally developed by Lewin (1946) and further developed by Schon (1983), Carr and Kemmis (1986) and Whitehead (1989), all cited in Baskerville and & Wood-Harper (2016). Towards the end of the 1990s the method began to become popular in scholarly investigations into information systems. One possible reason for its limited use prior to 1999 was that the approach

was characterised by a lack of consistent language as well as a lack of guidelines in respect of for its implementation and presentation (Davison, Martinsons & Kock, 2004).

7.5.1. Action Research

Information systems research has been widely criticised as lacking relevance (Davison et al., 2004; Rosemann & Vessey, 2008; Straub & Ang, 2011). This lack of relevance stems from the gaps between academic research and professional practice (Straub & Ang, 2011). According to Rosemann and Vessey (2008), action research represents the coincidence of action and research, or of practice and theory. Thus, according to the above definitions, action research leads to the production of new knowledge through practical solutions or improvements to real world problems. Baskerville and Wood-Harper (2016) are all of the opinion that the ability of action research to address the problem of relevance in IS research has led to its rise to prominence in the field.

There are numerous forms of action research. The most prominent of these used in information systems include participatory action research and canonical action research. The key difference between these two lies in the role of the researcher in the study. In participatory action research the research takes place within the researcher's environment and, thus, the researcher plays the dual role of participant and researcher. However, a researcher in canonical action research intervenes from the perspective of an outsider. This study took the form of canonical action research based on Davison, Martinsons & Kock's (2004) six core principles of canonical action research:

- There was mutual agreement between the researcher and the company regarding the objectives and anticipated outcomes of the research.
- The research involved an iterative process of problem diagnosis, planning, action, observation and reflection and documentation in order to ensure the research trustworthiness.
- The research was be guided by theory.

- The intervention resulted in changes that were directly related to the initially diagnosed problems.

Action research is clearly an ideal research method for validating and possibly refining information security compliance. In view of the fact that the aim of this study was not only to validate and possibly refine the information security compliance model, but also to study how the programme could be used to change employee behaviour, action research appeared to be the most appropriate method to use. This was in line with Walsham's (1995) assertion that action research is the ideal way in which to perform research in which the researcher is directly involved in the change action in an organisation.

Some researchers position action research as a subset of case study research although others, focus on the differences between the two approaches and, thus, appear to suggest that they should be treated as separate methods. The researcher in this study views them as different, however, that the reasons that make case study research viable are equally true for action research. The differences between action research and case study research are presented in Table 7.4.

Table 7.4: Case Studies vs Action Research (adapted from Vreede, 1995)

Case Study	Action Research
Researcher is observer	Researcher is active participant
Exploratory, explanatory or descriptive	Prescriptive, intervening
Focus on "How?" and "Why?"	Additional focus on "How to?"
May be positivist or interpretivist	Usually interpretivist

The original intention of action research is usually to effect change while carrying out research (Puhakainen & Siponen, 2010). Indeed, there is a continuum between the "describer" of case studies and the "implementer" of action research. In the middle is an "observer" is involved in social interaction with the participants and yet is not a participant. Such a research methodology is strong in the sense that it provides the researcher with both an inside and a working view of a case. The involvement of the

participants in the case also varies from those who become involved with the analysis and reflective learning to those who prefer only to act.

The action research approach taken for this study can be described by Baskerville and Wood-Harper's (2016) cyclical process as seen on Figure 7.5 (Baskerville & Wood-Harper, 2016). These phases include (1) identification of the problem, (2) planning an action, (3) taking action, (4) data analysis/evaluation and (5) future action planning. The exit stage represents the point at which the researchers believe they have obtained sufficient answers with which to address the research question(s).

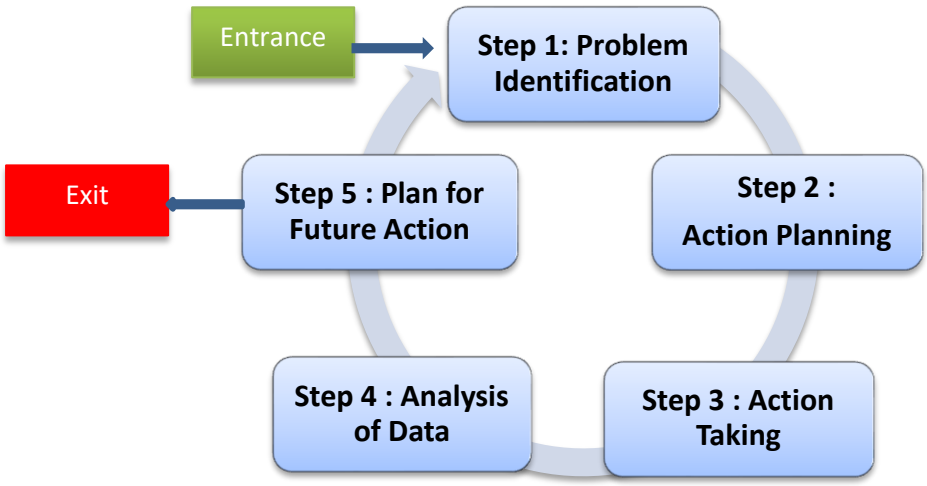


Figure 7.5: Five-Phase Self-Reflective Cyclical Process (adapted from Baskerville, 1999)

7.5.1.1. Problem Identification

During this stage the researcher identified a problem that triggered the desire for change. The diagnosis involved the self-interpretation of the complex problem exposed by literature. This interpretation was not through reduction and simplification but rather in a holistic manner. This diagnosis resulted in the development theoretical assumptions about the nature of the problem domain.

7.5.1.2. Action Planning

During this action planning the researcher specified actions that would relieve or improve the problems which had been identified. The formation of these planned actions was guided by the theoretical frameworks which indicated some desired behavioural changes possibility. In summary, the plan of action established the

behaviours to change, the approach to change the, and the assessment mechanism to track the changes.

7.5.1.3. Action Taking

Action taking refers to the implementation of the planned action. The researcher developed the framework discussed in chapter 6 then tested it as active intervention in an engineering SME in South Africa resulting in employee behavioural changes.

7.5.1.4. Analysis of Data/Evaluating

After the actions had been completed the researcher evaluated the outcomes. The evaluation was to determine whether the theoretical effects of the action were realised and whether the problems were alleviated. When the change was successful the process was critically reviewed to confirm whether the action undertaken, was indeed the sole cause of success. Where the change was unsuccessful, some changes on the framework were made for the next iteration of the action research cycle

7.5.1.5. Plan for Future Action

The plans for the future posed questions like: What will be done differently in the next iteration/action research as a result of this study? How will the findings of the study be reported so that they might be useful to others?

7.6. Data Analysis

Data analysis being the most complex and least understood aspect of the qualitative research process, Licthman (2013) suggests that the complexity lies within choosing the “right concepts” or in the belief that some findings are superior compared to others. It is therefore important that researchers’ not to fall for this notion as they will view one set of interpretations as more acceptable than another. The essence of qualitative research is using data to substantiate and strengthen the researcher’s position and not either to prove or disprove it. There is no right or wrong answer in qualitative research but rather acceptable explanations of phenomena based on the researcher’s experience. From an interpretive perspective, the researchers endeavours are to collect data through direct interaction with the people being

studied. The most important aspect of data analysis in this action research study was the search for meaning through the direct interpretation of what the researcher had observed as well as what had been experienced and reported by the employees who participated in the study.

Lichtman, (2013) define qualitative data analysis as working with the data, organising it, breaking it down into manageable units, coding it, synthesising it, searching for patterns, discovering phenomena of importance and communicating these as knowledge. In this study the researcher first concentrated on the entire data set, then attempted to decompose it and then re-constructed it into more meaningful information which could be used to make comparisons and contrasts between the patterns from the different iterations.

Strauss and Corbin (1990) describes qualitative data analysis in two stages, namely, open coding and axial coding. Open coding is concerned with the identification of categories or themes that emerge from the collected data while axial coding is concerned with conceptual model construction based on the emerging themes. This study made use axial coding to utilise evidence from the data to support the relationships between the conceptual model's constructs.

Leedy and Ormrod (2001) maintain that, during qualitative data analysis, the researcher starts by obtaining the raw data (structured or unstructured), organises and reduces the categories into groups and then compiles a final report. During the content analysis process in this study, the researcher collected and analysed qualitative data and followed the steps proposed by Leedy and Ormrod (2001) and as illustrated in Figure 7.6.

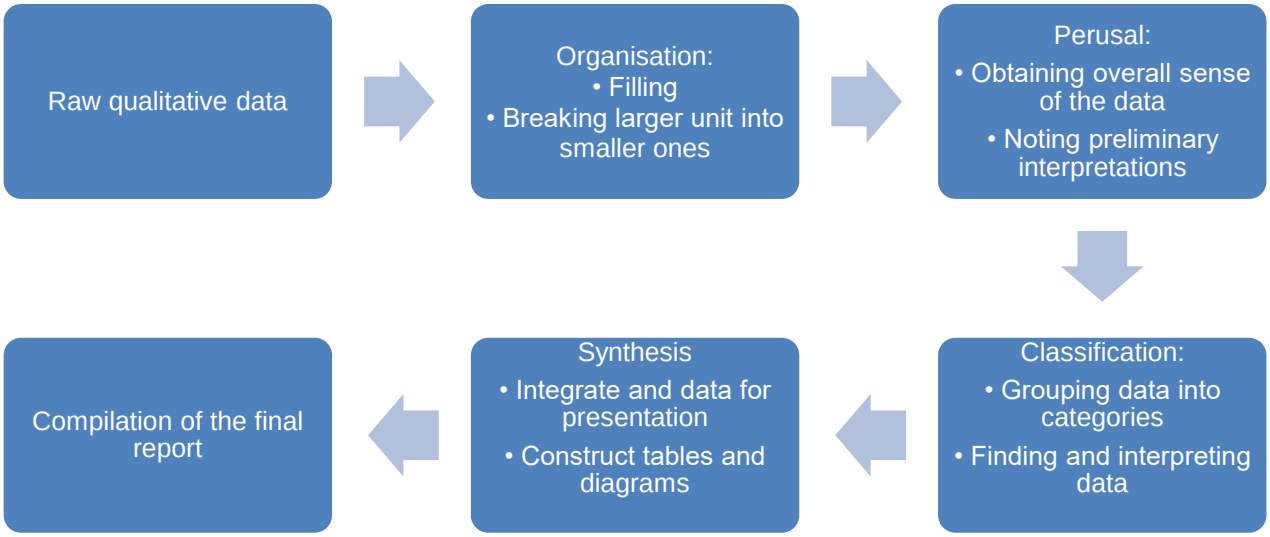


Figure 7.6: Data Analysis Spiral (Leedy & Ormrod, 2001)

In an action research study such as this study, the data collection and data analysis are conducted in an iterative manner with the results of the analysis in prior iterations helping to guide the subsequent collection of data. In this study the data collection and data analysis informed or drove each other, the iterative cycle was repeated and the data analysis design was checked and revised as the process continued.

7.7. Research Evaluation: Trustworthiness of the Study

The framework formulated and discussed was evaluated and refined through the expert review by nine experts from the field of information security and through action research. The action research which was conducted comprised four iterations. Traditionally credibility of research data is ensured by the following criteria, objectivity, reliability and validity. However there are usually only associated with positivist studies because they are often based on standardised instruments with may be assessed in a relatively straightforward manner. In the contrary, qualitative studies are usually not based upon standardised instruments and they often utilise smaller, non-random samples as compared to quantitative studies.

As a result it was not possible to strictly apply the evaluation criteria discussed above, because this study was specifically interested in questioning and understanding the meaning and interpretation of phenomena. Thus, these evaluation criterion would have and little or no value in this qualitative study.

Trustworthiness is the term which may be used in qualitative research to measure the quality of the research and it refers to the level to which the data analysis and findings are believable and trustworthy. It is difficult to assess the accuracy of qualitative findings. This study uses old but still relevant principles of trustworthiness from Guba and Lincoln (1981) and Krefting (1991) that suggest the use of four criterions namely, transferability, dependability, credibility and conformability. These are similar to the quantitative internal and external validity, neutrality and reliability.

7.7.1. Credibility

Credibility refers to the extent in which data collected and the analysis are believable and trustworthy. Credibility is the equivalent of validity in quantitative research. However, with regards to this research study, reality is relative to the context. Thus, this research may be valid only South Africa and not necessarily to others due to the social and environmental differences. The responsibility is with the reader to judge credibility of a research based on their social and environmental understanding of the study setting.

7.7.2. Transferability

Research findings are transferable or generalisable only if they fit into new contexts outside of the actual study context. Generalisability refers to the extent to which it is possible to extend the account of a particular situation or population to persons, times or setting other than those directly studied.

The major problem with transferability is the subjectivity of the key research instrument (researcher). However, to enhance transferability this research details the research methods, contexts and assumptions underlying the study in line with Seale (2004), who suggests achieving better transferability by providing a detailed, rich details of the settings of the studied in order to provide sufficient information to the readers judgement of the applicability of the findings to their own. In addition the

researcher was on high alert for possible biases and was conscious throughout the study of the possibility of multiple interpretations of reality.

7.7.3. Dependability

Dependability is similar to reliability in quantitative research. Dependability is concerned with getting the same results if the study was to be replicated under the same conditions.

For this study reliability assessment is tricky and it is also practically difficult as human behaviour changes depending on various influencing factors.,

Merriam (1998) suggests the following six strategies to enhance dependability in qualitative research:

- Triangulation – Use of multiple data sources or techniques to confirm the findings;
- Member checks – Taking data and tentative interpretations back to the participants from whom they were derived and asking them if the results are reasonable;
- Long-term observation;
- Peer examination;
- Participatory or collaborative modes of research;
- Clarifying the researcher's biases, assumptions, worldview and theoretical orientation at the outset of the study.

7.7.4. Confirmability of the Findings

Confirmability refers to the degree to which the research findings may be confirmed or validated by others. This is similar to objectivity in quantitative research. In order to make auditing of this research study by other researchers possible, all the data which has been collected was well-organised, archived and retrievable so that it may be made available to other researchers if the findings are challenged. Nine experts confirmed the validity of this study.

7.7.5. Triangulation

Triangulation arises from the need to confirm the validity of the processes used. It is an approach that utilises multiple data sources, multiple informants and multiple methods (e.g. focus groups, member checking, participant observation), in order to gather multiple perspectives on the same issue so as to gain a more complete understanding of the phenomena (Creswell, 2013; Patton, 1987).

Triangulation was the main approach that was used to evaluate the outcome of this study. Questionnaires (Survey tests) was the main primary data collection instrument. However other methods used included participant observation (with field notes), logs analysis and informal interviews. The outcomes of the questionnaires completed by the employees were triangulated with the results from participant observations, reports from log analysis as well as with the reports from the experts. The triangulation exercises were conducted at various levels in order to focus on a final outcome based on various perspectives.

7.7.6. Expert Evaluation

Lichtman (2013) argues against the need for experts to confirm the research's contribution in qualitative research as the researcher is likely to be the closest person to the actual research. However, for this study this was disregarded in pursuit to gain external opinions and advice. Nine experts were selected to engage in the evaluation of the framework and the research methodology. They were briefed on the goal of the study. Section 6.8 presents the ethical considerations which were taken into account during the study

7.8. Ethical Considerations

As this was a qualitative study the researcher had to interact with the employees, which meant entering their personal and private space. Understandably this raised several ethical issues that had to be addressed both during and after the research had been conducted. According to Creswell (2013), the researcher has an obligation to respect the rights and values of the participants. Miles and Huberman (1994) list

several issues that were considered for the collection and analysis of data for this study. Some of the issues considered include the following:

- Informed consent (Do the participants have full knowledge of what is involved?).
- Harm and risk (Could the study have a negative impact on participants?).
- Honesty and trust (Is the researcher being truthful in presenting the data?).
- Privacy, confidentiality, integrity and anonymity (Will the study intrude too much into group behaviours?).
- Intervention and advocacy (What should researchers do if participants display harmful or illegal behaviour?).

One unexpected ethical concern relating was respect for cultural sensitivity.

A appropriate steps were taken to ensure compliance to these strict ethical guidelines. In view of the above discussions, the next section describes how ethical issues were addressed during the course of this research study.

7.8.1. Informed Consent

The researcher informed the employees of the purpose, nature, data collection methods and extent of the research prior to the commencement of the study. In addition, the researcher communicated their typical roles. In line with this the researcher obtained their informed consent in writing in the format included in Appendix D.

7.8.2. Harm and Risk

As stated by Trochim (2000) the researcher guaranteed that no participants would be placed in a situation where they may have been harmed either physically or psychologically as a result of their participation in study.

7.8.3. Honesty and Trust

Adhering strictly to all the ethical guidelines serves as a standard in respect of the honesty and trustworthiness of the data collected and the accompanying data analysis.

7.8.4. Privacy, Confidentiality and Anonymity

In view of the fact that the study included a test-retest reliability check, total anonymity was not possible. However, the researcher ensured that the confidentiality and anonymity of the participants would be maintained by the removal of any identifying characteristics before the widespread dissemination of the information. The researcher also made it clear that the participants' names would not be used for any other purposes and nor would information that may reveal their identity in any way be shared. The integrity of data was protected by ensuring no manipulation.

7.8.5. Voluntary Participation

In addition to all the above mentioned precautions, it was made clear to the participants that the research was for academic purposes only and their participation in it was absolutely voluntary. In other words no one was forced to participate in the study.

Having discussed the research methodologies, research evaluation and ethical considerations, the next section concludes the methodology chapter of the study

7.9. Conclusion

This chapter outlined the research paradigm, research methodologies, strategies and research design used in the study, including the procedures, participants, data collection tools, data collection and analysis methods and data credibility issues. The research design used in the study was an interpretive action research. The data collected was analysed mainly through qualitative methods and using descriptive statistics. The chapter also briefly described the several stages involved in the design and development processes of the research in the study. The next chapter discusses the design principles and the Information Security Policy Compliance Reinforcement and Assessment Framework.

CHAPTER 8 - RESEARCH FINDINGS

Chapter 8:

This chapter presents a summary of the empirical data collected during the study. The chapter starts by discussing the methodological assumptions and then explains the position of the researcher in this action research study. The findings are then categorised and discussed. Some of the data was summarised by using diagrammatic representations such as bar and pie charts.

8.1. Introduction

Action research methodolgy is being increasingly used because it is grounded in action, aimed at solving an immediate problem situation and, at the same time, informs theory. Unlike other research methods, where the researcher seeks to study organisational phenomena but not to change them, the action researcher is concerned with creating organisational change and, simultaneously, studying the processes. Action research is strongly oriented toward collaboration and change and involves both the researchers and the subjects (Collis & Hussey, 2009). This research study involved four iterations of an action research at an engineering SME.

Engineering SMEs rely heavily on digital information stored on networked servers. This information includes patented and unpatented private and confidential designs, drawings and client information, all of which are vulnerable to security threats. However, SMEs tend to ignore the risk of the uninformed employee and are more concerned with vulnerabilities from external threats despite the fact that industry research suggests that the uninformed employee who is not behaving securely may expose the organisation to serious security risks such as data corruption, deletion and commercial espionage (Furnell, 2006; Furnell & Thompson, 2009; Krutz & Rusell, 2001; Sarkar, 2010; Wilson & Siponen, 2009).

This chapter discusses the processes and findings of the action research which was undertaken at the CEF. The rest of the chapter is laid out as follows. Firstly, the background of the organisation is discussed, after which the collection and analysis principles are explored. Finally, the findings of the action research are discussed.

8.2. Background

The action research for this study was conducted at a civil engineering SME in South Africa. In view of the fact that security is a sensitive issue the identity of the SME entity has been disguised and it was referred to as CEF. The action research empirical work aimed at refining and determining whether the proposed Information Security Policy Compliance Reinforcement and Assessment Framework would

actually be able to change employee compliance with the information security policy at the organisation and to assist in the creation and use of knowledge in a problem solving process. CEF was established in 1997. It develops designs, plans models and plans for its clients. The population of a study comprised every possible case that could be included in a study. The focus of the study was on all the employees at the SME, regardless of the positions they held or their experience. The action research described in this chapter of the thesis was conducted with all the employees of CEF – a total of thirty altogether – and it took place over a ten-month time period from February 2014 to November 2015. The executive of the organisation comprised five people, namely, the managing director, structural designs manager, geographical information systems (GIS) manager, physical and human resources manager and the water and sanitation manager. The organisation's technical team consisted of eighteen people while the other employees made up the office administration personnel.

The managing director owned the majority shares in the company. In addition, he had been formally defined as executive manager in the organisation and, as such, was responsible for the decisions on most engineering, economic and administrative issues. The technical team was responsible for most of the design drafting and product development issues while the physical and resources head was responsible for human resources, corporate ICT and IS resources and issues.

CEF had invested considerably in the research and development of the this proposed framework. According to the organisation's management, the resulting innovations should play a major role in compliance with the organisation's information security policy as the organisation's values included protecting both customer and business partners' information. This was the main reason why the management of CEF had welcomed the development of a companywide information security campaign. However, this had not had to be done from scratch as an information security policy and end-user instructions were already in place. All the employees had signed it on

induction, although very few of the employees remembered doing this and also did not remember the contents of the documents. Thus, the researcher was able to establish that the employee awareness of information security issues was at a very low level.

On the other hand, it appeared that the organisation's executive assumed a relatively high level of employee awareness as it advocated that the employees read and understand the policy when they signed it. They were, however, puzzled by the high incidences of violation of the organisation's security policy. The policy stated that all employees should adhere to safe practices when using any corporate ICT, equipment or information. The managing director described the situation in the following way:

"I have noticed that, although employees have read the information security policy, they still don't always behave securely and the reason for that still remains a mystery" (Personal Communication, Managing Director of CEF, January 2014).

After serious discussions with the researcher, the organisation's managing director came to realise that the negative security behaviours could, indeed, be due to lack of information security understanding. This led to the researcher being granted permission to embark on action research. The managing director would benefit by all his employees being educated on sound security practices and by the statistics of the awareness levels that would emerge while the researcher would benefit from the opportunity to validate, refine and test the models in a real life scenario. CEF was selected as a host organisation for the empirical exploration of the framework because it exhibited the characteristics of a typical engineering SME. In order to achieve organisation-wide changes in compliance, it was important that as many employees as possible became involved in and committed to the change process. The size of the company made it possible to interview all employees informally several times during the research process. This allowed rich interaction between the employees and the researcher and, consequently, detailed information on their

compliance and/or non-compliance with the information security policies and instructions.

8.3. Methodological Assumptions

For the purposes of this action research project, each employee at CEF was deemed to be an active processor of the information he/she received. Hence, he/she was regarded as capable of deciding personally whether or not to comply with the organisation's information security instructions, such as the email policy. In addition, it was noticed that this decision was affected by an employee's social environment. It was expected that information security policies and instructions would not be obeyed without their reasonableness being questioned. Hence, the study also incorporated relativist ontology (Guba & Lincoln, 1981). i.e., multiple realities socially constructed by each employee were assumed. For this reason, interaction between the researcher, executives and other employees was regarded as necessary in order to create a joint construction of the prevailing situation and to design solutions for the potential problem areas. This joint construction was vital if the study's goals of increasing the level of compliance with the organisation's information security policy were to be achieved.

8.4. Research Strategy and Position of the Researcher

In this action research study the researcher was an outsider to the organisation and, hence, not a participant and researcher at the same time. This study was, thus, in fact, a canonical action research study. However, the researcher was also not regarded as an objective, passive outsider. The organisation's management and the other employees expected him to play an active role in planning, designing and delivering the training programme and evaluating the results. Thus, the researcher became responsible for planning and implementing the information security awareness training programme. In addition, the researcher acted as a consultant. The researcher's involvement may, at best, be described as *expert involvement* as the researcher was regarded as an expert among the collaborators. Some of the

tasks were individual tasks although cooperation between the researcher and the collaborators was also an essential component of the research process.

8.5. Principles of Information Collection and Analysis

Information was collected and analysed constantly throughout the research process. Four methods were used for collecting the research data, namely, (1) informal interviews, (2) online questionnaires, (3) participatory observation and (4) a survey of logs (antivirus, firewall and incident logbook). The goal of the information security awareness training programme was to increase the employees' compliance with the organisation's information security policy and, thus, information on their previous skills, knowledge and behaviour was collected.

The questionnaires were used for collecting information related to the employees' knowledge, attitude and behaviour regarding information security. The information gathered was then used to evaluate whether the employees possessed the knowledge required for complying with the security policy. Informal interviews were also used to gather information on motivational factors related to compliance with the policy. In addition, these informal interviews were used to collect the information required on the employees' skills and knowledge in respect of the subject matter and to evaluate the results of the interventions.

The employees were interviewed using normal social interaction techniques. The information was recorded by means of field notes. Initially, the researcher had considered using an audiotape to record the interviews as this appeared to be the most useful way in which to avoid follow-up questions and show respect for people's time. Furthermore, it would have helped to capture the information in the participants' own words. However, despite these advantages, the use of an audio recorder was abandoned. The reason for this was to make the participants feel more comfortable and relaxed and more willing to present their own opinions and perceptions.

Whenever any doubts about the meaning of an interviewee's statements arose, this was verified immediately during the interview. Further verification was also carried out during the data analysis phase whenever this was deemed to be necessary in order to avoid incorrect interpretations. A major issue with interviews is that the questions are easily influenced by the researcher's perceptions, perspectives, interests and agendas. However, in order to avoid this, the researcher asked questions that were relatively neutral. This was deemed necessary so as to diminish the extent to which the participants' perceptions may have been governed by frameworks of meaning unintentionally imposed by the researcher.

The researcher initiated discussions with 'grand tour questions' that were sufficiently broad to enable the employees/participants to describe their situations in their own words. The aim of these questions was to provide focus without giving direction or suggesting forms or types of responses (e.g., "Tell me about information security relating to your work processes"). Other forms of global questions included questions on what was typical (e.g., "How does your group typically act with regard to email encryption?") and on specific matters (e.g., "Describe what you did last time you received an email with an attachment from an unknown sender?"). The researcher then presented sets of questions, either typical or specific, that focused on concepts which had already been mentioned (e.g., "You earlier mentioned that this policy is difficult to comply with"). This was done in order to obtain more detailed information about issues that had already been covered. During all the phases of the interview, the researcher adopted a neutral stance and wrote down the responses as accurately as possible.

Following the approach discussed above, all thirty employees at CEF were interviewed once or twice during the action research process. Informal group interviews were also conducted, especially during lunch times when everyone was in the canteen. The aim of these informal group interviews was to identify the themes that had emerged from the information and to ascertain whether these themes

supported the theories on compliance with information security instructions. The data analysis formed the basis for the refinement of the framework. In addition, the employees' behaviours were observed in normal working situations. These observations were recorded in a field note for observations.

The researcher and the company director at CEF closely monitored the findings of each iteration throughout the study to get insight of directions to take. Necessities realised throughout led to the researcher uploading large amounts of material onto the corporate intranet, including the organisation's security manual, security audit reports, memos of meetings and risk analysis reports.

8.6. Conducting Action Research at CEF

Exploring a theory-based Information Security Policy Compliance Reinforcement and Assessment Framework that aimed at increasing the level of compliance with the organisation's information security policy by finding out and helping to overcome the constraints that prevented the employees from complying with the policy corresponded with the typical aim of action research, namely, finding solutions to concrete problems in practice (Argyris, Putnam, & McLain Smith 1985). Action research aims at simultaneously promoting both the theoretical conceptualisation and practical command of the phenomena of a study. In other words, action research aims to help examine theories and concepts critically in the light of action, and change existing ways of working. Accordingly, the researcher decided that action research was as an appropriate approach for the practical refinement and evaluation of the models proposed

Although action research is typically considered as an interpretive research approach, positivistic empirical indicators may also be used (Hofstee, 2006). These indicators included measurable indicators of the employees' improved security behaviour such as a decrease in the number of malware infections. However, as behavioural changes are not always easy to measure, it was decided to also use interpretive methods to gather the requisite research data. One possibility was to

interview the employees in order to find out whether training had made any impact on their motivation, attitudes and behaviour while another method was to use surveys which utilised a likert scale (e.g., five-point continuum from strongly disagree to strongly agree).

8.7. The Action Research Events

The action research started with planning, continued onto execution, observation and reflection and then returned to planning a new cycle. The planning itself typically relates to a social or practical problem rather than a theoretical question. The researcher attached importance to the values, beliefs and intentions of the participants in the study as he attempted to change the social reality for the better into an emancipatory frame of reference. Participants need to be actively involved in the research process, sometimes to the extent that they become co-researchers.

Table 8.1: Action research activities

	Processes carried out
Iteration 1	1. Assess compliance using behavioural intention 2. Run awareness and training campaigns 3. Assess compliance using behavioural intention
Iteration 2	1. Assess compliance using behavioural intention 2. Run awareness and training campaigns 3. Assess compliance using behavioural intention
Iteration 3	1. Assess compliance using the proposed Model for Information Security Compliance Assessment
Iteration 4	1. Reinforce compliance using deterrence 2. Assess compliance using the proposed Information Security Compliance Assessment Model

The total duration of the action research totalled eleven months. This eleven month action research consisted of four cycles with approximately three to four months

between each cycle. Table 8.1 summarises the activities involved in the four iterations.

8.8. Findings

The findings of the online questionnaire provided a background to as well as an insight into the information security awareness levels of the organisation's employees while the participant observation allowed the researcher to gain first-hand experience of the employees' behaviour in real life situations. The informal interviews which were conducted provided details of the employees' feelings towards information security and, finally, the document surveys highlighted the occurrence rate of security breaches over the study period.

Once data had been collected, it was important to process it and transform it into meaningful information. The data was weighted in the interests of a better reflection of the overall employee security compliance level than may otherwise have been the case. ENISA (2007) argues that the less processing the better. Each organisation needs to find the right balance for itself. There is no "one-size-fits-all" solution. The weighting in this study was decided upon with the managing director, the IT team leader and the resources head of the organisation, who all agreed that the intention conversion measure (weighted 50%) was the most important measure, followed by the behavioural intention measure (weighted 35%) and, lastly, the competence measure (weighted 15%). Although this is not a fixed way of weighting it was, nevertheless, the weighting that was best for CEF.

However, SMEs that adapt this framework should formulate their own weightings that suit their situation and environment. The information was processed using the matrices presented in Table 8.2 and as agreed upon by the researcher and the organisation's management.

Table 8.2: Information Security Measures Weightings

Competence Assessment (15%)	Intention Assessment (35%)	Intention Conversion Assessment (50%)
Number trained (8%)	Knowledge (15%)	Antivirus statistics (10%)
Training frequency (2%)	Attitude (3%)	Incident logbook (10%)
Pass and fail rate (5%)	Behavioural intentions (17%)	Observations (30%)

The results and importance weightings were processed in a spreadsheet application and the output was presented in the form of tables, graphs and awareness maps in accordance with the method used in the study by Kruger and Kearney (2006). The findings of the empirical study are summarised in Table 8.3.

Table 8.3: Findings of Information Security Competence Measurement Iterations

	Competence Assessment (15%)	Intention Assessment (35%)	Intention Conversion Assessment (50%)	Total
Iteration 1	N/A	18	N/A	51%
Iteration 2	N/A	30	N/A	86%
Iteration 3	13	32	23	68%
Iteration 4	13	33	44	90%

Table 8.4 depicts shows the scale that was used to interpret the level of compliance. This scale was adapted from that of Kruger and Kearney (2006), and modified to take into consideration the recommendations made by the organisation's managing director.

Table 8.4: Awareness Level Measurement (Kruger & Kearney, 2006)

Awareness	Measurement (%)
Good	75–100
Average	60–74
Poor	30–59
Very Poor	30 and less

The findings of this study are now discussed per iteration and then also per the method used.

8.8.1. Findings of the Action Research Events

8.8.1.1. Iteration 1

This iteration comprised three activities.

(1) Assess compliance using behavioural intention

It serves no use to have an information security policy in place that addresses awareness if it cannot be monitored and compliance with the policy enforced (Von Solms & Von Solms, 2004). Compliance assessments help SMEs to identify vulnerable areas. It is then essential to ensure that these areas are addressed as soon as possible by an information security awareness programme. Hence the first step involved assessing the employees' initial information security compliance level before any awareness intervention was initiated in order to ascertain the starting information security compliance state.

This assessment was conducted based on Kruger and Kearney's (2006) assessment model. This model assesses performance measures which are the collective role of attitudes, knowledge and behaviours. The employees completed an online questionnaire in the form of a test (please refer to CD in Appendix B). However, their scores were not linked to their names to ensure their anonymity, even to the management of the organisation.

(2) Run awareness and training campaigns

The second activity involved implementing awareness campaigns. Awareness and training increase employee knowledge and this, according to the underpinning theories, should convey the management's (subjective norm) position on security. These theories also relate knowledge to belief and attitude alterations. This was important because it was to be done based on the Model for Information Security Awareness and Training which formed part of the Information Security Policy Compliance Reinforcement and Assessment Framework presented in this study (Chapter 7). This would then help to refine and evaluate its effectiveness by means of a comparison of the initial compliance assessment with the assessment conducted after this awareness campaign.

The information security awareness communication path used was E-learning. E-learning has grown significantly over the past several years as technology has been integrated into education and training. E-learning may be defined as instruction which is delivered electronically via the internet, intranets or multimedia platforms such as CD-ROM or DVD (Smart & Cappel, 2006). An e-learning system was used in this study instead of the conventional classroom style because it provided a configurable infrastructure that integrated learning material, policies and services into a single solution to the quick, effective and economical creation and delivery of awareness and training content. E-learning allows employees to train at their own convenience and learn at their own pace. It has also proved to be cheaper in terms of time and money rather than bringing everyone together.

The e-learning awareness and training programme for this study was designed and developed by the researcher with the assistance of a multimedia designer and a web page developer and by using Macromedia Flash, Macromedia Dream Weaver, PDF, PowerPoint, Access, Gold wave, and Photoshop software in order to present the programme material in both a visual and an auditory format. The programme material was presented in the form of a website containing information based on the weaknesses which had been identified in the initial assessment. It also included

relevant information security topics such as viruses, phishing, email safety, passwords and social media. All the pages contained attractive information security pictures/videoclips/jokes in an effort to create a more relaxed e-learning environment. The employees participating in the study received an email with instructions on how to use the awareness and training programme, including the link to the awareness and training website. The website for training and awareness was constructed as follows (please refer to Appendix B for a copy of the website):

Figure 8.1: Snippet of Awareness Website Used

The home page: This page contained an introduction to information security and the motive behind the awareness and training. The employees needed to be motivated as to why information security was important. The home page then linked to the awareness pages.

The awareness pages: These pages supplied information on topical issues and examples of breaches. They also contained all the information security information required by the employees.

The assessment page: This page was used as the data collection tool for acquiring data from the employees, which was then used to measure their information security awareness levels.

(3) Assess compliance using behavioural intention

The assessment was based on Kruger and Kearney's (2006) assessment model. This assessment aimed at establishing the extent to which the Model for Information Security Awareness and Training had managed/failed to increase compliance within the organisation. In order to obtain this insight the pre-intervention assessment was compared to the post-intervention assessment. This assessment involved finding out whether the procedures and processes that were implemented within an organisation were working as they should and if they were being complied with. This was to ensure that the information security policy had been properly implemented and all information had been secured (Danchev, 2003). The objects assessed were identical to those assessed in the initial assessment and the same questionnaire was used. The questions in the questionnaire were grouped according to the following categories as proposed by Kruger and Kearney (2006), namely, knowledge, attitude and behavioural intent.

8.8.1.2. Iteration 2

The activities carried out in iteration 2 were identical to those in iteration 1. Iteration 2 was carried out because the compliance levels had increased but not to the levels as had deemed to be safe by the researcher and the organisation's management.

(1) Assess compliance using behavioural intention

In addition to the reason for this iteration, it is important that information security awareness compliance is monitored regularly to ensure that employees are keeping abreast of the ever evolving technology. Today's state-of-the-art may be obsolete tomorrow (Williams, 2002; Kritzinger, 2006) and, hence, it was vital to ensure that all the employees were up to date with all the latest technologies adopted by the engineering SME and that they knew how to use them in a secure way.

(2) Run awareness and training campaigns

The frequency of information security awareness campaigns (time period) is widely debated among professionals (Johnson, 2006). It may range from quarterly to bi-annually to annually and will differ from one organisation to the next according to an organisation's specific security needs. However, many specialists maintain that the more often such campaigns are run, the better. In other words, implementing an information security awareness programme should not be seen as a once-off action but rather as an ongoing commitment to securing information by both old and new employees (Danchev, 2003). Hence the awareness campaigns were also conducted during this iteration for the aim of keeping the employees abreast of technological advancements. These awareness campaigns also addressed the issues which had been picked up in the first assessment of this iteration.

(3) Assess compliance using behavioural intention

Subsequent to the awareness intervention in the second iteration, the same assessment instrument which had been used in the first assessment was administered to the same respondents to observe whether there had been any changes in compliance after the intervention.

8.8.1.3. Iteration 3

After the third iteration both the researcher and the management were satisfied with the levels of employee knowledge, attitude and behavioural intents. However, it was surprising to find that compliance with the information security policy was still an issue. This finding led to the development of the Model for Information Security Compliance Assessment and its addition to the framework presented in the study, which also took into account intention conversion. The aim was to try to factor in the behavioural intents that do not convert into actual behaviours and, thus, to provide a more accurate assessment of the security position of SMEs in terms of the employee aspect. This iteration consisted of one assessment activity only which included informal interviews (Appendices C), observations and documents/log report analysis

8.8.1.4. Iteration 4

This iteration comprised two activities. This iteration was aimed at reducing the gap between intention and actual behaviour that had been unveiled during the third iteration. This led to the addition of the development and addition of the Model for Employee Information Security Compliance Motivation and Reinforcement to the proposed framework in an attempt to bridge the gap between intention and actual behaviour by reinforcing the conversion of intention into actual behaviour through deterrence techniques.

The first activity in this iteration involved implementing an awareness campaign that included being rewarded by secure behaving and being punished for unsecure behaviour. In consultation with the researcher the management decided to include information security aspects in the organisation's overall yearly employee rating. In addition, management also introduced a certificate and yearly awards for sound security behaviour. These initiatives functioned as deterrence factors. After this initiative an assessment based on the Model for Information Security Compliance Assessment was conducted in order to evaluate the effectiveness of the Model for Employee Information Security Compliance Motivation and Reinforcement.

8.8.2. Findings of the Online Questionnaires

The study collected qualitative data through online surveys which were six times in four iterations (see Figure 8.1). The first round of the data collection took place during the needs assessment and then during iterations 1 to 3, as discussed in the preceding chapter. The information collected was used to assess the information security compliance of the employees and also to identify knowledge gaps that would need to be addressed in the subsequent information security awareness campaigns and training. The four online surveys contained different, although similar, questions. Although the surveys contained different questions, the surveys all had a similar structure as they were measuring the same attributes i.e. knowledge, behaviour and attitude. Please refer to CD-ROM in Appendix B for the survey structures and questions.

The use of qualitative methods was important for studying the dynamics of the intervention as qualitative research provides an understanding of social processes (Strauss & Corbin, 1990; Denzin & Lincoln, 2011). The aim of the qualitative evaluation of the intervention was to measure the information security awareness levels of the employees, identify knowledge gaps and assess whether the intervention was making any progress in the intended employee behavioural intention moulding. The qualitative data collected through the online surveys was analysed by looking for patterns in the data that described how the intervention had been interpreted and why the intervention had either modified or failed to modify employee awareness and skills. In addition, the data was also analysed in an attempt to ascertain the reasons for such patterns.

8.8.3. Findings of the Participant Observation

Participant observation is fundamental to any action research study. The involvement of the researcher in this type of observation may vary from complete observation to complete involvement (De Vos, Strydom, Fouché, & Delport, 2005). For the purposes of this study the researcher's participation in this scenario was an equal mix of observation and involvement. The researcher's observations at CEF were focused on employee behaviour in respect of information security awareness.

The observations relevant to this study centred on one particular instance, namely, the computer network of the organisation became very slow as a result of a virus. This resulted in major losses as production was very slow for three days while there was no production at all for one day when the server and computers were being scanned and cleaned. It was then discovered that, although every computer on the network was equipped with an antivirus, most of the employees had turned the antivirus off as they reported that their computers had become slower. They had also deleted some email attachments. The virus was assumed to have entered the organisation's computer network through one of the computers on which the antivirus software had either been uninstalled or disabled. It had then duplicated itself on all

the other computers and the servers. This had slowed down the server to such an extent that it took more thanr 25 minutes to log on to the network. It would take over an hour to retrieve a 1.5MB document from the server, so was saving a document of the same size. It had taken the computer technician an entire day to get rid of the virus. The antivirus software was also updated and reactivated on all the computer resources. This issue was typical of the problems encountered at the organisation. The researcher also believed that these problems were exacerbated by the lack of security knowledge.

Although firewalls and antivirus software were in place, information security awareness and training was needed to ensure that the employees used these correctly. This required the collaboration of all employees.

The researcher also observed that the employees kept their passwords underneath their keyboards on notes or else pasted behind their screens. They also shared their passwords with their spouses and among themselves. On several instances employees came in with their spouses and children and allowed them to use the organisation's computer resources. Also, when an employee was absent from work, their colleagues would telephone the employees to ask for the login credentials so that they could log in although this was not necessary as their own login credentials were sufficient to enable them to log on to the system.

8.8.4. Findings of the Document/Log Survey

In qualitative research observations and interviews are the conventional methods used for data collection and the benefits of the document survey are often neglected (De Vos et al., 2005). The documents required for this type of study included the minutes of meetings, agendas and office memoranda that pertained to security breaches (De Vos et al., 2005).

The researcher intended to obtain documentation from CEF (the action research study organisation) to obtain insights into the occurrences of and solutions to the

information security breaches that the organisation had encountered. In particular, the researcher was interested in documented evidence of viruses, identity theft, phishing attacks and physical security breaches.

However, despite several attempts to establish the existence of the required documentation, no such information was forthcoming and, thus, this proved not to be a feasible source of data for the study. The researcher's efforts to find these types of documents proved fruitless.

8.8.5. Findings of the Informal Interviews

Interviewing is the most significant data collection method used in qualitative research (De Vos et al., 2005). Kvale (1996, cited in De Vos et al., 2005) views interviews as an attempt to comprehend the participants' point of view and to extract meaning from their descriptions of experiences.

Interviews were conducted during both the needs assessment and also during all the iterations of the action research. The purpose of the interviews was to ascertain the extent of the information security knowledge of key employees. The findings from the interviews are discussed below. The findings from the needs assessment online survey helped the researcher to compile a list of topics that were then addressed in the first round of the information security awareness and training.

Interviews were conducted with the managing director, resources head, one administrative staff member, five technical employees and one temporary staff member. The participants chosen were representative of the small workforce of the company and were relevant due to the roles they had played in the observations discussed above.

The participants were informed of the goal of the research study and were given the background of the field of information security. They were asked pre stryctured questions to make them comfortable and open ended there then asked. In addition,

the participants were encouraged to discuss other issues relating to the questions and that had that emerged during the assessment test.

8.8.5.1. Respondents in the Informal Interviews

(i.) **Managing Director**

The Managing Director of CEF is involved in all aspects of the organisation and he is aware of every issue that occurs in the administrative and technical environments. Both the nature of the organisation and the managing director's role in the organisation require that he be on hand to assist in finding a solution so as to prevent any stoppages in production. When a problem arises, employees always refer the situation to the managing director in order to find a solution.

(ii.) **Resources Head**

The resources head is involved in all aspects of the resources (human and computer) in the engineering production environment. She reports to the managing director when a problem arises and is responsible for the majority of the work required to ensure a solution is found. In other words, the resources head carries out most of the problem-solving activities.

(iii.) **Technical Employees**

The five technical employees chosen to participate in the interviews included two engineers, one CAD operator (draughtsman), one GIS operator and the IT technician. All IT-related problems are reported to the IT technician. These five technical employees, with the exception of the IT technician, have little responsibility to ensure that these problems are resolved.

(iv.) **Administration Staff Member**

The administrative staff members of CEF are not actually involved in the engineering aspect of the organisation but are involved in the marketing and tendering process. However, in view of small nature of the organisation, the administrative staff do play an important role in problem-solving situations related to information security and privacy issues.

(v.) Temporary Employee

The temporary staff member had been recruited on temporary basis to assist in the implementation of a new civil engineering software package. However, this employee was available for 3 months of the research. The employee was asked questions only relating to his/her experiences at CEF.

8.8.5.2. Interview Responses Summary

The questions asked during the interviews were open ended. Field notes were also taken. There were 10 questions that were posed randomly to the employees. The responses to these questions are summarised in Table 8.5.

Figure 8.2: Interview Response Summary

Security Policy
1. Does this organisation have a formal information security policy in place?
• The temporary employee said he was not sure, the managing director said yes and the rest said no although there is one in place. • The human resources department had a signed copy of the document by each employee.
2. Do you think you have sufficient knowledge and skills to ensure that you behave securely when using the organisation's ICT resources?
• In general the respondents indicated that they felt that they possessed sufficient information security knowledge and skills. • The administrative employee, however, felt that she could benefit from some training.
3. Do you think the organisation is doing enough in terms of the physical protection of the information asset?
• All the participants were happy with the physical security, citing that there were burglar gates, an alarm with rapid response and CCTVs were installed in all the offices and passages.
4. Do you think the organisation is doing enough in terms of the technological protection of the information asset? (Firewalls, antivirus software, anti-adware, etc.)
• Only three participants knew what firewalls were. However, all of them knew that they had antivirus software installed on their computers but claimed that it slowed their computers down. • The majority of them indicated that they did not check whether their antivirus was up to date.
5. Do you think you should be part of the organisation's information security initiatives?

• Most of participants felt that security was both complicated and time consuming and that the ICT technician should be responsible for security and not them.
6. Is there any system in place to measure the success of and/or compliance with the security policy in this organisation?
• The majority of the respondents believed that the CCTVs on the premises were to spy on them and, hence, they felt compliance was being monitored. • Most of them indicated that compliance was mandatory and that failure to comply may result in disciplinary action.
7. Do you think the information on the server may be of any value to someone other than your organisation?
• All answers had in common that the respondents were of the opinion that their competitors would love to know their cutting edge secret.
8. Have you ever made any mistake that posed a security threat to the information asset?
• The majority indicated that they felt they behaved securely although one admitted having once opened a website that had a virus but that it had been detected by the antivirus software.
9. (a) Do you take any information/laptop home so you can work over weekends/at night?
• Most of the participants responded in the negative with the exception of the managing director who indicated that he took his laptop home every day.
(b) Do you have a password on the flash drive or computer that you take home?
• The managing director said he had a password on his laptop in case it was stolen. The answers of the other participants were irrelevant as they did not take any either data or equipment home.
10. Do you sometimes use your work computer for personal things, e.g. internet banking, online shopping and social networks?
• Everyone answered in the affirmative. However they also indicated that most sites, especially social networks, were blocked so they did not use it that much.

8.8.6. Findings of the Expert Review Process

This section describes the process in which the research project and its main contribution were critically analysed by nine experts in the field of information security in three distinct rounds. The expert review was conducted in parallel to the action research with the feedback from each round serving as a refinement of the research contributions analysed in each subsequent round. The framework was reviewed by three of the experts when it was developed and then by another three experts after the modifications to the framework after the second iteration. The final expert review

was conducted by three more experts after the modifications of the framework after the third iteration.

These nine experts were approached and requested to conduct a critical analysis on the main contribution of the study, the Information Security Policy Compliance Reinforcement and Assessment Framework, the theoretical background and evaluation of the methodology.

Each of the experts was given the link to the online expert review questionnaire (please refer to Appendix C). In addition, they were also given another link to a brief informative presentation of the study (please refer to the CD-ROM in Appendix B). The details of each round of the review process are discussed below:

8.8.6.1. Expert Review Process: Round 1

The response from the reviewers in this first round were summarised and used to further develop and refine the study. The main recommendations and the results obtained from this round included the following:

- An expert asked how behavioural intention is related to actual behaviour. This led to the researcher clarifying the assumption that behavioural intention is almost equal to the actual behaviour.
- An expert questioned whether the framework would also change the behaviour of the malicious insider. As a result, in order to remove any possible confusion the study then highlighted that it would focus on the uninformed employee only, although the malicious employee is equally dangerous.
- An expert highlighted that the study had included certain very old literature references and sources and, thus, they felt that the problems highlighted could have long been solved. This impacted negatively on the overall credibility of the study and, therefore, these sources were replaced with more up-to-date and credible literature sources.
- It was pointed out by one of the experts that the study lacked focus in certain areas and did not link the risks posed by the employee to a lack of knowledge.

Literature highlighting the risks of the naïve insider and relative statistics were then included.

- The experts indicated that the framework diagram provided excellent guidance. However, they did feel that, in certain aspects, the diagram was unclear and unreadable. The diagram was then redrawn and improved accordingly.

8.8.6.2. Expert Review Process: Round 2

After the first round of the expert review process, the research was updated and, after three months, a second round of review was conducted. Three different experts were selected. Their comments and opinions were then received, summarised and implemented accordingly. The key responses received from these experts included the following:

- An expert pointed out that some of the statements made about the framework were either worded incorrectly or were unsubstantiated, such as the comment that “Intention is not equal to behaviour”. This resulted in the researcher finding supporting literature. The researcher also removed all claims that could not be substantiated and correcting the wording to ensure that it conveyed the correct meaning of the statements.
- It was also identified that the study needed to emphasise its final contribution as it lacked the required focus. This led to more discussion on the final contribution of the research project i.e. the models. It was made clear that the main contribution of the study was artefacts in the form of models.
- It was also suggested that the study should better justify the underpinning theories. As a result, explanations about why the Theory Planned Behaviour, the Knowledge Attitude Behaviour Theory and the Deterrence Theory had been chosen and related to the research project were included.

8.8.6.3. Expert Review Process: Round 3

After another four months a third round of assessment was conducted. Three more experts were consulted and requested to review the proposed framework. Their responses included the following:

- A particular expert requested that a better, more specific definition of an insider be included in the research project as the concept had not been described correctly and in sufficient detail. For example, whether temporary workers or consultants are insiders. Thus, a definition specific to this study was formulated.
- All the three experts agreed that the introduction and the explanation of the framework had been sound but that its limitations were not clear. Thus, the framework was revised, expanded upon and a more comprehensive discussion drafted.
- An expert found the name of the framework, namely, “Information Security Policy Compliance Reinforcement and Assessment Framework” misleading as the focus of the study had been on compliance only and little had been discussed in terms of policies. However, the name was not changed as this would have broadened the scope of the research.
- An expert questioned why, after the awareness and training initiatives had been introduced, the study had assessed compliance and not awareness. This led to a revision of the research to point out that measuring awareness involves assessing knowledge retention only and not necessarily behaviour.

8.9. Conclusion

Ensuring that the employees knew and cared about information security was definitely a challenging task. Identifying the themes emerged from the data helped in the crafting of a cohesive, professional awareness website that would enable employees to instantly recognise the message. Determining the concepts which employees should understand was a priority as efforts focused on the topics that were lacking but which were critical to safeguarding the organisation’s information

security asset. Finally, repetition was vital in conveying the message. Security awareness messages were conveyed on a regular basis and in a variety of mediums to ensure maximum exposure to the messages. Regular assessments revealed the effectiveness of intervention efforts and also allowed for adjustments to the message focus and method of delivery in order to obtain the best results for the SME environment.

As agreed upon by the management and the researcher the employees who had participated in the study received a certificate confirming that they had completed the requirement as per their managing director's directive. It was also decided that these security awareness training certificates would be valid for one year only. As such, the employees would have to undergo training on a yearly basis. The topics and questions would, however, change yearly so that no one took the same test twice. Once the certificate was nearing its expiration date the employee would merely log back into the system, review the information, and complete the assessment again. Since this was to be done on a yearly basis most of the employees said they did not mind having to complete the training and testing process again. In addition, favourable responses were received indicating that the uploaded information was found to be very useful.

This chapter contained a discussion of the findings of the research study as they related to the research problems presented in Chapter 1. The aim of the proposed framework was to assist organisations to implement information security assessments in a manner that would assess actual employee behaviour towards the protection of information assets rather than just employee intentions to protect. As such, a framework to ensure information security compliance and promote acceptable information security behaviour was designed, evaluated and refined through expert review and action research.

The findings from the document/logs survey, participant observation online surveys and the informal interviews were presented. The participant observation revealed both password sharing and antivirus software disabling while the online surveys provided the data that was analysed to provide a measure of the information security awareness during all the iterations. These online surveys were in the form of tests which each employee had to complete to earn an information security awareness certificate which was valid for one year (see discussion in the preceding chapter). The informal interviews were a rich source of information for identifying the state of the information security at CEF before any intervention took place.

In conclusion, the analysis of the literature study and the feedback from the expert reviews as well as the action research iterations results provided the data required to develop a refined framework. This framework was designed essentially to help both to reduce the risks that employees pose to organisations and to move towards a positive information security culture. This was supported by the agreement of all the experts and also those involved in the discussion, development and refinement of the framework. The next chapter contains a discussion of these this study's findings.

CHAPTER 9 - DISCUSSION AND CONTRIBUTION

Chapter 9:

This chapter contains a detailed discussion of the findings presented in Chapter 8. These discussions were aimed at critically analysing the findings while linking the interpretation of the findings to the unique developmental context of the study. The basis of these discussions was the theoretical foundation which was found in relevant literature.

9.1. Introduction

While prior research reveals a growing concern that security awareness campaigns are not achieving the desired compliance, this may be attributed to two factors, namely, flaws in the awareness campaigns and/or flaws in the assessment tools used. Nevertheless, the gap between knowledge and behaviour as a result of flaws in the assessment tools has not been widely researched. This research project explored the information security threats to which employees expose the organisations they work for through their behaviour, information security intention and behaviour gap as well as the difficulties involved in assessing employee information security compliancey. These problems were the focus of the research questions presented in Chapter 1. The research objective of the study was also presented in Chapter 1 and was aimed at minimising the extent of these problems. The solution comprised a proposed framework (as detailed in Chapter 6), namely, the Information Security Policy Compliance Reinforcement and Assessment Framework. This framework illustrates the relationship between information security awareness, knowledge, behavioural intent and actual behaviours. The framework was evaluated and refined through an expert review process and action research (see Chapter 8). This chapter presents a summary of the key findings from the data analyses discussed in Chapter 8 and the preceding chapters on the literature review and discusses the implications of these findings. The discussions in this chapter are aimed at linking the research questions with the proposed framework, the findings while relating the interpretation of the findings to the theoretical foundations which was discussed in the literature review.

9.2. Discussion of Findings

It is difficult to conduct a value-free social inquiry (Patton, 1987) as the researcher may unintentionally introduce his/her values and preconceptions into the inquiry and this may inevitably influence the researcher's approach to the study. In an attempt to reduce this inevitable bias, rigorous steps were taken during the data collection, including the use of mixed methods in this interpretive study. Detailed records of the

action research iterations, data collection instruments and field notes used in the study were maintained. The researcher was dependent on these detailed records of the data analysis in order to limit subjectivity in the reporting of the research findings.

9.2.1. Discussion of the Action Research Findings

The findings in the previous chapter are summarised in both Table 9.1 and Figure 9.1 and are discussed in the next sections. This discussion comprises 4 sections according to the 4 iterations in the action research.

Table 9.1: Summary of Findings

	Competence Assessment (15%)	Intention Assessment (35%)	Intention Conversion Assessment (50%)	Total
Iteration 1	N/A	18	N/A	51%
Iteration 2	N/A	30	N/A	86%
Iteration 3	13	32	32	77%
Iteration 4	13	33	44	90%

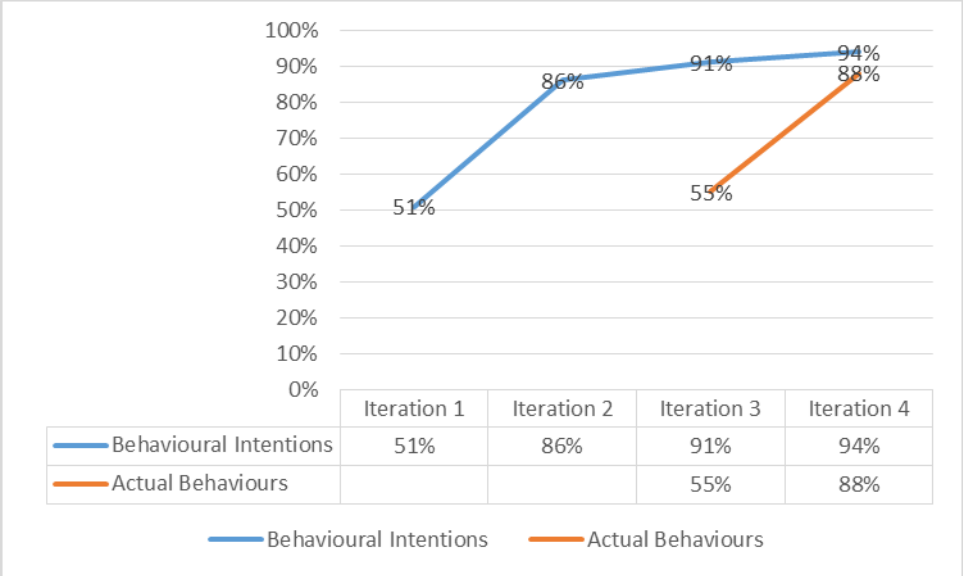


Figure 9.1: Behavioural Intentions vs Actual Behaviours

The assessments highlighted the employees' compliance or intention to comply as well as their training needs. Regarding the first iteration of the action research, the measurement revealed that the employees did not possess an adequate

understanding of identity theft, encryption, viruses and spyware, thus highlighting certain topics for the purposes of awareness and training. These results also justified the concerns of management as well as the need to allocate resources to information security awareness and training.

9.2.1.1. Iteration 1 Discussion

This iteration was used as a needs assessment to assess the prevailing state of information security compliance and the areas that needed to be addressed. During this iteration of the action research, Kruger and Kearney's (2006) assessment tool was used to assess the employees' security compliance. This tool does not assess either competence or intention conversion and, thus, it was not applicable in Table 9.1. However, the tool does infer that behavioural intentions will equal actual behaviours. As shown in Table 9.1 the average behavioural intention score of the employees was 51% (18/35 X 100). In other words, this needs assessment revealed a lack of both awareness and information security knowledge.

9.2.1.2. Iteration 2 Discussion

Table 9.1 showed that, after the first information security awareness and training initiative, there was an increase in the intention measures from 51% to 86% (30/35 X 100), thus indicating a significant improvement in information security knowledge and intention. However, employee actions needed to match the awareness levels and the organisation's management reported little or no change in actual behaviour. This highlighted that behavioural intentions do not reliably lead to actual behaviours.

9.2.1.3. Iteration 3 Discussion

This iteration tried to obtain a more accurate sense of the security compliance. During this iteration the proposed employee information security compliance assessment tool was used. The intention measure increased from 18% to 33% (first-second iteration). This was primarily a result of the increase in information security knowledge. The minimal increase in attitude was mainly because attitude is also

affected by other organisational factors which are not related to information security, such as job satisfaction.

The behavioural intent measure changed from 86% in the second Iteration to 91% (32/35X100) in the third iteration. However, this assessment was not based on intentions but also on competence while the conversion of intention into behaviour measures was also considered. These additional measures lowered the overall security assessment delivered in the third iteration to 58%, which was 28% lower than in the previous iteration.

9.2.1.4. Iteration 4 Discussion

During the fourth iteration the employee information security compliance assessment was used again. The competence measure did not change as compared to the previous iteration because there was no change in the number of employees trained, no change in the training frequency and the pass rate remained steady.

During this iteration the intention conversion measures increased from 32 to 44% after an information security reinforcement procedure of penalties and rewards had been implemented. Table 9.1 compares actual behaviours to behavioural intentions during iterations 3 and 4 of the action research. The results demonstrated the bias of behavioural intentions in terms of assessing information security competence, thus giving an overly optimistic, pseudo picture of compliance.

9.2.2. Discussion of Research Questions Findings

The main research question posed was:

How can SMEs in emerging economies reinforce employee information security policy compliance?

This main research question was broken down into three sub-research questions and the main research question was then answered by addressing these three sub-research questions.

9.2.2.1. Sub-Research Question 1

Is there a gap between employee behavioural intention and actual behaviours concerning the information security policy?

It was found that behavioural intent with regard to compliance with ICT security policies was somewhat directly proportional to all components of the KAB and TPB. While this finding was consistent with the theories, it was found that the relationship was not equally proportionate. For example in the third iteration of the study, there was a 15% increase in knowledge that led to a 12% increase in behavioural intent which in turn cultivated a 5% increase in actual behaviours. This revealed a gap between intention and actual behaviours. There are, however, a limited number of empirical studies that have explored the relationship between behavioural intention and actual behaviours in the context of information security.

9.2.2.2. Sub-Research Question 2

How should SMEs motivate or reinforce the conversion of behavioural intentions into actual behaviour?

This study provided evidence that rewards and/or punishments have an important role to play in the context of reinforcing employee compliance with information security policies. Such rewards had a significant impact on the employees' decision to comply with ICT security policies. The inclusion of information security as part of the employee yearly ranking in the 4th iteration of the study revealed a 32% increase in the conversion of behavioural intentions into actual behaviour. This was because security compliance was now contributing to performance bonuses and promotions and, thus, compliance would result in positive rewards while non-compliance would result in the opposite.

9.2.2.3. Sub-Research Question 3

How should employee information security compliance be assessed taking into account the gap between intentions and actual behaviour?

This study revealed that the assessment of actual behaviour should be based on the following.

- A competence assessment which is related to the competence aspects of information security assessment, such as number of employees trained, frequency of training and pass rates.
- An intention assessment which addresses the intention assessment aspects such as knowledge, behaviour and attitude.
- An intention convention assessment which assesses aspects such as antivirus statistics, incident logs and observations.

The aspects measured by the information security compliance assessment model produced insights into the effectiveness of security interventions. After the third iteration, although behavioural intentions where at 91%, actual behaviours were still at 55%, thus revealing that compliance with the policy was still an issue. However, this result also revealed the effectiveness of actual behaviour assessments.

9.3. Recommendations to the Organisation

Given the initial lack of standardisation, the recommendations to CEF were intended to guide them or any other similar organisations on the way in which assess and ensure information security compliance.

- There is a need to document and record the lessons learnt from problem situations in order to apply these lessons to future situations to avert further costly delays.
- The organisation may benefit from the creation of a “yellow pages” application which would direct employees to the necessary expert should a problem occur, e.g. a computer has a virus or a security breach is suspected. This would reduce the time spent searching for the relevant expert to assist with the problem.
- Furthermore, in order to remain abreast of the ever-changing information security technologies and risks posed by the employees, it is advisable to run needs assessments every 12 months.

- Employees operate on feelings, moods, etc. that are ever changing and, hence, the conversion of intentions into actual intentions is dependent on several psychological factors. However, if the motivation for compliance has failed, in order to ensure such conversion, enforcement strategies should be considered to assist in combating omissive behaviours.

9.4. Relevance and Validity of the Action Research at CEF

The action research conducted at CEF tested the relevance, feasibility and applicability of the proposed framework. The goal was to refine and evaluate the real life applicability of this framework. The proposed framework was intended to assist in moulding employee behaviour by providing relevant assessments. It was, thus, important to first explore how the security behaviour of employees could be improved. Whenever a solution to a problem was thought to have been found it was necessary to verify, refine and evaluate it.

Action research is known to be a suitable research strategy for initial evaluation and the possible adjustment of an approach. In addition, action research aims to help the participants to investigate reality in order to change it. This was also the goal of this study as it was hoped that the study would result in organisation-wide changes to the prevailing practices. It is for these reasons that action research was selected as the most appropriate research strategy for the purposes of the study.

The action research intervention at CEF took place in a multivariate social situation. All the employees of the company were involved with varying relationships between them. In addition, the research involved the complex business relationships between CEF and its customers and partners. These relationships created the need for thier increased security as it was necessary to protect CEF's innovations as well as the customers' and partners' sensitive information. The prevailing situation inside the organisation was also complex as many of the employees considered that management was passive about promoting information security issues. This made

the prevailing situation at CEF challenging from the point of view concerning this intervention.

9.5. Evaluation

Research evaluation is a necessary step in order to ensure the credibility and integrity of a research project. Oates (2006) proposed a set of equivalent criteria for both positivist and interpretivist research. These are presented in Table 9.2.

Table 9.2: Quality in Positivist and Interpretivist Research (Oates, 2006)

Positivism	Interpretivism
Validity	**Trustworthiness**
Objectivity	**Conorganisationability**
Reliability	**Dependability**
Internal validity	**Credibility**
External validity	**Transferability**

In view of the fact that this was an interpretivism study, the following interpretivist criteria applied to this research study:

1. **Trustworthiness:** The trustworthiness of the experts which were consulted to validate and refine the proposed model was evaluated. The experts used in this process were respected in their respective field. They were also selected from the field of information security management research. Thus, the recommendations made by these experts were deemed to be trustworthy.

2. **Conorganisationability:** This criterion was met through the use of multiple data collection techniques, culminating in the action research and expert review in order to conorganisation the outcome of the research. The action research findings conorganisationed the theoretical findings and this led to the development of the refined framework which was also conorganisationed through expert reviews.

3. **Dependability:** Dependability is established through the use of the work of recognised writers in the relevant literature as well as the contribution of experts in the field of study in the form of the expert review. The use of established theories and models that have been evaluated in a number of research projects contributed to the dependability of this project. The theories and models used in this study included: TPB, the KAB theory and DT.

4. **Credibility:** Credibility was achieved through the use of multiple data collection techniques (triangulation) and also the use of expert review (as described under conorganisationability).

5. **Transferability:** Transferability was achieved as the research model may be applied to other inter-organisational settings with similar characteristics to CEF e.g. another SME Engineering firm in South Africa.

Through the application of these five criteria, the findings of this research project may, therefore, be considered credible.

The use of these evaluation methods meant that it may be stated that the research project may be considered to have met the requirements of action research and, thus, it is a valid action research project.

9.6. Conclusion

Employees in SMEs are faced with the same security threats as those faced by employees in larger organisations. However, unlike employees in larger companies, they are disadvantaged because, in the main, they have limited access to sources of information (e.g. training) that could improve their awareness of the information security threats to which they may be exposed. In determining the *'Employees intention to comply to information security policies',* the employee knowledge about information security related terms and threats was found to be poor at CEF where the study was conducted. The employees' intention to comply with the policies increased

only after the awareness campaigns that included mugs, posters, mouse pads and online learning. An interesting observation was made was that employees' attitude towards information security was more positive in areas where they appeared to be more knowledgeable about information security concepts or principles.

The overall intention into behaviour conversion of the employees at CEF was also found to be poor. A closer analysis of behavioural intent revealed that, in some areas (e.g. password lock) improved knowledge, coupled with a positive attitude, was associated with positive information security behavioural intention. However, the positive correlation found between awareness and behavioural intention was not sufficient to achieve acceptable compliance levels. Hence, the use of deterrence in the form or punishment and rewards was found to be necessary to increase compliance. It was interesting to note that the punishment threat yielded better compliance as compared to rewards for good behaviour. The four action research cycles evaluated the theoretical foundation of the proposed framework and confirmed its applicability to the employee information security compliance context. The next chapter provides an overview of the study in the form of concluding remarks.

CHAPTER 10 - CONCLUSION

Chapter 10:

This chapter contains the concluding remarks to the overall study. This is followed by an explanation of the way in which the research questions were addressed. The objectives of the study and the contributions made to the greater body of knowledge by the study are then outlined. Finally, the research limitations and suggestions for future research are detailed.

10.1. Introduction

Information communication and technology (ICT) has, for some time, been advancing globally in the context of SMEs. However, the progress in South Africa, which is an emerging economy, has been somewhat slow although it is now catching up at a rapid rate. Unfortunately, however, this is accompanied by security risks. This study explored the security risks associated with employee information security compliance in an emerging economy (South Africa). However, while the experience of SMEs in an emerging economy may be unique, the threats which both employees and the SMEs face are not unique. Several researchers in the field of information security, for example, Öğütçü, Testik and Chouseinoglou, (2016) and Peltier, (2005) consider employees to be the most vulnerable and to constitute the weakest link in information security. Information security awareness has been promoted as the best measure to counteracting the threat posed by employees with awareness being used to influence both behaviour and compliance. However, unlike many other studies, this study recommends the assessment of employee information security compliance and not just awareness or behavioural intent as some employees, despite having been trained and being aware of how they should behave, simply do not behave in the way in which they should. This is termed omisssive behaviour or the intention-behaviour gap. This gap is not usually apparent to the organisations themselves as their assessment tools do not assess actual behaviours but, instead, they assess intentions and/or information security knowledge retention.

In order to address the problem of poor information security compliance assessment tools resulting in false compliance levels, this study suggests the assessment of actual behaviour to supplement behavioural intentions. It also suggests reinforcing the conversion of intention into actual behaviours by including deterrence methods in the usual motivational approaches. This approach introduces punishments for unsecure behaviours and rewards for secure behaviours. It is similar to that used in the traffic law context where a transgressor is fined for undesirable behaviours.

The previous chapter discussed the findings, recommendations and contribution of the study. This chapter summarises the overall research project by focusing on the achievements and evaluation of the study. The framework presented in the study (chapter 6) was based on secondary data collected from a review of existing literature on information security policy implementation and compliance assessment methods while the primary data which was used to evaluate the proposed framework was collected by means of a questionnaire, logs survey, interviews and observations. The feedback from these was used to refine the framework. In addition, the framework was also evaluated and refined through an expert review process. This chapter highlights how the research objectives were met in order to answer the research questions posed in the study. The chapter also discusses the theoretical framework; the research methodology used; and the limitations of study. Finally, the chapter offers recommendations for future research.

10.2. Summary of the Literature

It is well documented in the literature that the information security precautions being carried out focus primarily on reducing the risk of outsiders trying to access an organisation's information assets. The literature further reveals that, although the outsiders pose a risk, the insiders pose almost the same risk but that few or no precautions are being taken against the risk posed by insiders. It is, however, far more difficult to detect unsecure security behaviours on the part of employees as technical controls usually focus on detecting outsider intrusion (Peltier, 2005).

The literature has also revealed significant information security problems that affect employee behaviour in respect of complying with information security policies. This exposes the employees themselves and the organisation to a wide range of vulnerabilities such as viruses, social engineering scams and the improper usage of the corporate information assets. These vulnerabilities comprise weaknesses that are specifically targeted by outsiders who are trying to gain access though unsuspecting insiders. A detailed study of the literature was conducted in order to identify these

vulnerabilities. The literature has revealed that information security awareness may go a long way in providing protection against these vulnerabilities.

It is a fundamental requirement that regular interventions be carried out to increase employee awareness and competence and, thus, encourage compliance intention (Furnell & Thomson, 2009; Cox, 2012). If such competence drives are effective, a security-aware culture will emerge and good practice will become the norm. Such an information security-aware culture will also minimise the risks to information assets by reducing the risk of employee misbehaviour and harmful interaction with information assets (Van Loenen, 2015).

However, having run awareness drives and delivered training, organisations are often unable to accurately assess whether employees are applying their knowledge with the required level of assiduity (Kruger & Kearney, 2005). According to Kruger and Kearney (2006), organisations should measure the employees' information security knowledge, their attitudes towards information security and, lastly, their behavioural intentions. Unfortunately, however, there is no agreed upon framework of what to assess or how to assess it (Kruger & Kearney, 2008). The majority of assessment models assess only the employees' reception and retention of the acquired knowledge and implicitly assume that such knowledge will inevitably lead to secure behaviour. However, this assumption is unsubstatiated.

The KAB theory, TPB and DT, as identified in the literature, assist in explaining how employees intend to behave and also the elements that influence their actual behaviours.

10.3. Review of the Research Questions

The study aimed to answer the following research question:

How can SMEs in emerging economies reinforce employee information security policy compliance?

In order to answer the main research question, three sub-research questions were identified. Table 10.1 summarises the research objectives of the study and indicates the chapters in which they were discussed.

Table 10.1: Research Objectives and Chapters in Which They Were Addressed

Research objective	Chapters	Research approaches
Is there a gap between employee behavioural intention and actual behaviours in respect of the information security policy?	2, 3, 4, 8	Literature review and conceptual analysis
How should SMEs motivate or reinforce the conversion of behavioural intentions into actual behaviour?	4, 6, 9	Conceptual analysis, constructive research and theory testing with action research
How should employee information security compliance be assessed taking into account the gap between intentions and actual behaviour?	4, 5, 6, 9	Literature review, conceptual analysis and theory testing with action research

1. Is there a gap between employee behavioural intention and actual behaviours concerning the information security policy?

This sub-question was addressed in Chapters 2, 3, 4 and 8. The theories that explain employee behavioural intentions and behaviours were identified, namely, the TPB, KAB theory and DT. The theoretical basis assisted in the formulation of the proposed behavioural intention model and also assisted in establishing an accurate and logical argument to support the proposal of this model.

2. How should SMEs motivate or re-enforce the conversion of behavioural intentions into actual behaviour?

This sub-question was addressed in Chapters 4, 6 and 9. During the literature review current information security compliance motivation techniques used were examined and their weaknesses discussed. The use of deterrence factors was introduced in Chapters 4 and 9. The discussion on deterrence techniques showed that employees tend to behave as prescribed by their intentions only if there is no cost to behaving in this way or if they are being rewarded for secure behaviours. It was highlighted that the cost of a punishment or a reward may contribute significantly to the conversion of intentions into behaviours. This sub-question was also discussed in Chapter 6 where it was explained how the proposed model for motivating and reinforcing the conversion of intentions into behaviours will assist in achieving information security compliance.

3. How should employee information security compliance be assessed taking into account the gap between intentions and actual behaviour?

Chapters 4, 5, 6 and 9 addressed the last research sub-question. Chapter 4 examined 'Push and pull' persuasion techniques while Chapter 5 discussed methods use to assess these persuasion techniques. Chapters 6 and 9 discussed the proposed information security compliance assessment model. This model highlighted various aspects of measurement and explained ways in which measurement should be conducted within the context of information security compliance.

10.4. Theoretical Foundation

Three theoretical backbones were used to explain the behaviour of employees towards information security, namely, the TPB, the KAB Theory and DT. According to the researcher's review of literature in this area, no prior information security research has used all three theories in a single information security study. Although research has been carried out in the area of information security compliance, there is little on the intention-behavioural gap in information security on the basis of psychological theories as well as a lack of any description of the theory/theories underlying these methods. Psychology is the science of the mind and behaviour.

Social psychology has been used for several research projects in the area of education, learning, human behaviour and information systems (Hogg & Abrahams, 1988).

10.4.1. Theory of Planned Behaviour

TPB posits that employee behaviour is driven by behavioural intentions, where behavioural intentions are a function of the employee's attitude toward the behaviour, the subjective norms surrounding the performance of the behaviour, and the employee's perception of the ease with which the behaviour may be performed (behavioural control) (Ajzen, 1991). According to TPB, the stronger the behavioural intention, the greater the likelihood that it will convert into actual behaviour. Information security assessment is considered to be a behavioural issue and, thus, it was appropriate to base this study on the TPB. However, in order to further clarify the constructs of the TPB the study also drew from the KAB theory.

10.4.2. Knowledge Attitude Behaviour Theory

KAB evolved from behavioural intention and cognitive processing theories. Its main goal is to facilitate those factors that lead to behaviour. KAB is deemed to be an influential explanatory theory for predicting employees' intentions to behave securely (Da Veiga & Eloff, 2010; Parsons et al., 2010). Information security awareness and training instil knowledge into the employees and also assist in engendering attitudes which, when combined, may help an employee to formulate his/her behavioural intentions (Kruger & Kearney, 2005). However, these theories lack a practical relationship between actual behaviour and behavioural intentions.

10.4.3. Deterrence Theory

In order to overcome the problem of employees' negligent ICT security policy compliance, the use of sanctions, grounded in Deterrence Theory, is widely advocated by both practitioners and ICT scholars. Deterrence Theory, which may be traced back to Bentham (1748-1832) and Beccaria (1738-1794), posits that individuals weigh costs and benefits when deciding whether or not to commit a crime and they choose crime only when it pays. In other words, if an individual believes that

the risk of getting caught is high (certainty of sanctions), and severe penalties will be applied if one is caught (severity of sanctions), then Deterrence Theory posits that such an individual will not commit a crime.

10.5. Overview of the Research Methodology

This section summarises the research methodology used in the study. The various paradigms used in research were presented and this study followed an interpretivist approach, in terms of which expert reviews were conducted during the review process. In addition, the study took the form of an action research. Action research allows for simultaneous practical problem solving and the refinement of scientific knowledge. This goal implies two important process characteristics: Firstly, interpretive assumptions are made about observation and, secondly, the researcher intervenes in the problem setting. This study represented a detailed example of an action research process of design together with the process that should be followed when designing an information awareness programme. The reason why action research was chosen as the most appropriate approach in this research project was explained as were the reasons for using expert reviews.

Expert reviews formed part of the primary data collection and assisted with the analysis and provision of feedback that was useful for the evaluation and refinement of the proposed framework. The reason why expert reviews were selected as the primary source of data collection for this study was because experts in the information security domain possess valuable and implicit knowledge that is difficult to obtain via other means. This knowledge included much expertise and insight into the processes and important design aspects that was required in the development of the information security process and behavioural intention model. This type of knowledge is difficult to transfer and, therefore, through these reviews, a greater understanding of the problem was obtained than may otherwise have been the case. The expert reviewers were approached with flexibility, thus allowing the experts the freedom to respond according to their unique opinions and judgements by means of

open ended questions like: “in your opinion what are the flaws of the research methodology used for this study?”

This study acknowledges the difficulty to measure the dependability of the responses received from the experts. The dependability is heavily reliant on the experts review process, their position and expertise, the situation, expectations and own perceptions on the subject. The expert review process was, therefore, conducted in a non-leading manner using defined research data that was presented for analysis and with the aim of ensuring that the process remained as open as possible.

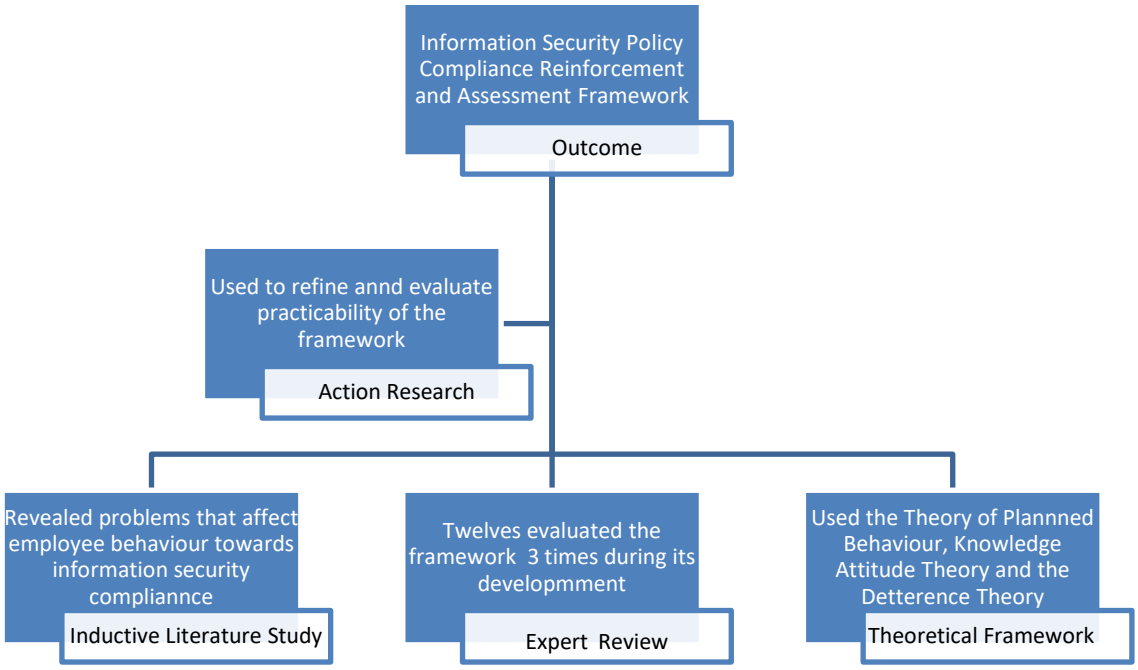


Figure 10.1: Research Methodology Overview

The overview of the research methodology is summarised in a bottom up approach in Figure 10.1

10.6. Results and Findings

The main objective of this study was to develop, present, refine and evaluate a Framework for Information Security Compliance Reinforcement and Assessment.

During the first and second iterations of the action research, Kruger and Kearney’s (2006) assessment tool was used to assess the employees’ security compliance.

After the first information security awareness and training initiative there was an increase in intention measures from 51% to 86%. This provided a sound indication of an improvement in information security knowledge and intention. However, employee actions needed to match the awareness levels and the organisation's management reported little or no change in actual behaviour. This highlighted how behavioural intentions do not reliably lead to actual behaviours.

During the third and fourth iterations the employee information security compliance assessment tool introduced in this study was used. The overall security assessment delivered by the third iteration was at 58%, which was 28% lower than the previous iteration. This was primarily the result of the inclusion of the competence and intention conversion measures in the compliance assessments. The competence measure did not change for the last two iterations because there was no change in the number of employees trained, no change in the training frequency and the pass rate remained steady.

The intention measure increased from 18% to 33% (first–second iteration), mainly as a result of the increase in information security knowledge. The minimal increase in attitude was mainly because attitude is also affected by other organisational factors which are not related to information security, for example, job satisfaction.

The intention conversion measures increased from 23% to 44% after an information security reinforcement procedure of penalties and rewards had been implemented. However, this procedure was beyond the scope of this paper and will not be discussed here.

Additional discoveries were that, even although, initially, the employees' security knowledge levels at CEF were very low, they had demonstrated a positive attitude towards securing the organisation's information asset. However, they did not possess the skills and knowledge required to behave in a secure manner. This also helped to

show that, as was revealed by the literature, the risk to which employees expose an organisation is often the result of genuinely unintentional naïve mistakes,.

It was disappointing to note that, although knowledge increased dramatically during the iterations, the increase in attitude was marginal. However, this was probably because the employees had a certain attitude towards the organisation and it was not possible to change this attitude through information security awareness alone.

The findings of this study support the TPB, KAB and DT theories. The awareness campaigns were aimed at communicating the organisation's information security policy. This was in turn intended to increase employee knowledge, alter attitudes and cultivate a positive behavioural intention. The behavioural intention would then be reinforced into actual behaviour as a result of the fear of or attraction to rewards as imposed by DT.

After releasing the final findings of the study, CEF's Managing Director stated that *"I now believe that my employees lacked the knowledge to behave securely. Furthermore, I believe that there are employees who did not understand the risks and the possible consequences of their poor security practices. In addition, even after acquiring knowledge, some employees seemed to lack motivation to abide by the organisation's information policy. However, making it part of their yearly evaluation made them take it seriously".*

10.7. Evaluation and Validation of the Research

After the refinement of the research project during the expert review process and a more thorough investigation during the action research, a refined framework was developed which sought to provide organisations with a framework to use when assessing and reducing the intention-behaviour gap in information security compliance initiatives.

The evaluation of the study is reflected in detail in the research methodology of the approach used. Nine experts in the security field were presented with the findings of the research and requested to comment on the correctness and applicability of these findings to the research problem so as to enable the researcher to further refine the artefact which had been developed. Expert review is a popular method that is widely used and generally accepted to gather data from respondents. The technique is designed as a collective communication process which is aimed at a group of individuals and with the objective of obtaining a wide variety of expert opinions on specific real-world problems. The expert review conducted in this study consisted of four rounds of review, analysis and feedback.

The first iteration was validated by three experts who provided an extensive critical review of the assessment model and its concepts. They had questioned whether the proposed framework would either change or assess the behaviours of malicious insiders. A second iteration of the evaluation process resulted in less extensive but highly valuable feedback from a different set of three experts. The opinions and comments obtained from this iteration were found to be extremely influential in terms constructive criticism and resulted in a successful improvement of the proposed framework on all levels. Finally, the third iteration produced strong agreement and consensus from the experts consulted and who were given the opportunity to respond. Throughout the review process all the responses and comments made were taken into account and applied to the research where applicable.

The research data that was presented to the experts was continuously and thoroughly refined after each round of review, thereby ensuring the increasingly credible standard of the study.

The secondary data collected included literature on frameworks, methodologies, online journal articles and other internet sources, past research projects, surveys and books. The initial literature review was performed in order to determine the research

problem and research objectives. This was very important as it identified the body of knowledge on which the study would be based and which it would expand upon.

De Vos et al. (2005) note that dependability and trustworthiness are important in a document study. To ensure and increase the dependability of the document study conducted in this study, only the work of well-known researchers, authors and institutions were used in the construction of the theoretical framework. In general, it may be said that this study was both credible and dependable.

10.8. Contributions

The primary contribution of this study is the development of the Framework for Information Security Compliance Reinforcement and Assessment presented in Chapter 6. Fundamentally this framework and its theoretical foundations extended the body of existing knowledge by introducing the ability to:

- Map the gap between knowing and doing;
- Map the effects of awareness intervention on employee awareness over a period of time,
- Assess employee competence and assess employee intention to behaviour conversion.

The knowledge domain framework in Figure 10.2 classifies research contributions into four categories and this study is classified as an improvement of solutions/new solutions for known problems.

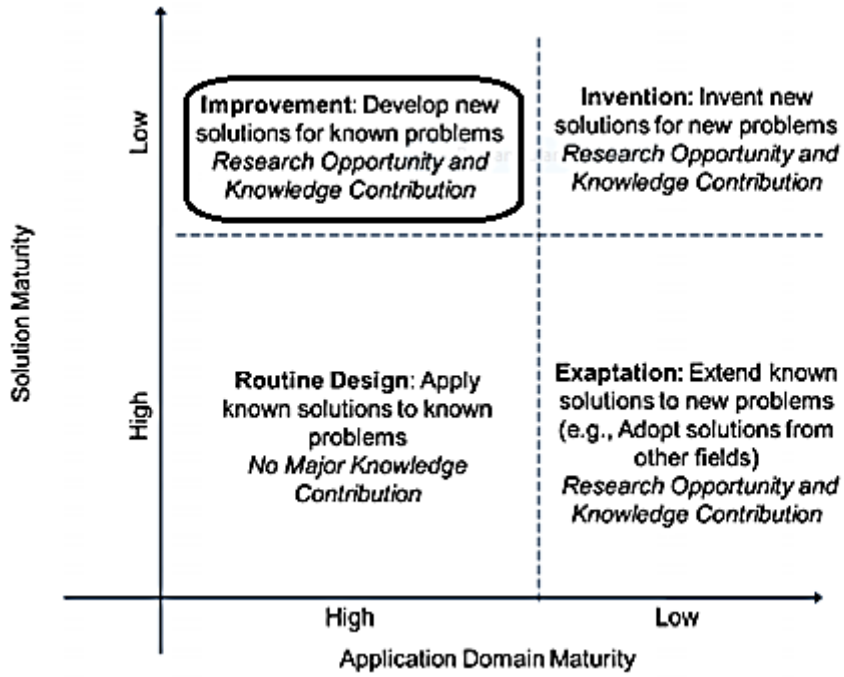


Figure 10.2: Knowledge Contribution Framework

In order to realise the study's primary objective, the following key processes were followed:

1. Determine whether a gap exists between employee behavioural intention and actual behaviours concerning the information security policy.
2. Identify methods for motivating or reinforcing the conversion of behavioural intentions into actual behaviour.
3. Establish how employee information security compliance should be assessed, taking into account the gap between intentions and actual behaviour.
4. Evaluate and refine the framework by means of expert review and action research.

This study may be also be said to have made significant theoretical contributions as outcomes after meeting the research objective. This is discussed in the following section.

10.8.1 Theoretical Contribution

The majority of information security awareness and compliance studies that have been conducted focused on employee knowledge retention and behavioural

intention. However, this study explored the less researched area of employee information security compliance within engineering SMEs in an emerging economy.

10.8.1.1 Evaluating Theory

In an attempt to explain employee behaviour in respect of information security, prior studies have tested the social bond theory, protection motivation theory, TPB, TRA, KAB theory and DT (Kruger & Kearny 2005; Herath & Rao 2009; Safa et al. 2016, Posey et al. 2014; Ifinedo, 2012).

This study contributed to the existing body of knowledge by evaluating three behavioural theories, namely, TPB (Ajzen, 1991), KAB theory (Kruger & Kearney, 2006), and DT (Beccaria, 1963). As proposed by these theories, this study confirmed the existence of relationships between attitude, behavioural intent, knowledge, behavioural controls, rewards and punishments with actual behaviours. The replication of the theory is discussed in the next section.

10.9. Recommendations for Further Research

This study focused specifically on the methods for assessing compliance and closing the gap between intention and behaviour in a specific setting. It would, however, be interesting to see the results of the same research in a different setting, for example, a different country or an SME in a different industry. This research study used only deterrence as a method of reinforcing. However, the researcher acknowledges the existence of other psychological methods. Thus, instead of awareness initiatives, future research could start with deterrence initiatives and ascertain whether it is possible for deterrence to achieve compliance without knowledge.

According to Lee, Lee and Kim (2016), excessive focus on the reinforcement of information security may place employees under stress and this reduces productivity. It would be both interesting and worthwhile to investigate the effects of information security reinforcement on productivity.

Future research could also address the shortcomings highlighted in this research. Thus, studies that develop theory-based cognitive and behavioural information security compliance approaches are recommended. In addition, the practical efficiency of such approaches should be empirically explored. This is valid for all cognitive approaches. This thesis presented research agendas for information security compliance and assessments based on the TPB, the KAB theory and DT. In terms of the behavioural approaches, rewards and punishments have not been thoroughly explored in the context of information security and, hence, studies that empirically explore their practical efficiency would be welcome.

Finally, this research study explored the risks posed by omissive behaviours on the part of naïve employees and revealed the knowing and doing gap. This is a relatively new aspect in the field of information security and one that has significant potential of resulting in e-security behavioural initiatives. Further exploration of the risks posed by the malicious insider as well as the outsider is also recommended. This research study could have focused on these aspects as well although this may potentially uncovered countless other areas of interest in this context which would have made the study difficult to manage. However, this does mean that there are further research possibilities. This study was conducted in a specific environment and focused on a particular population group and, thus, it is not possible to assume the generalisability of the results. The strengths and limitations of the study are discussed in the next section

10.10. Strengths and Limitations of the Study

The researcher believes that this study has made a contribution to information security compliance research. In particular with regard to moulding the behavioural intentions of employees in SMEs into actual behaviours, it is also hoped that the study has shed light on compliance assessments. In addition, it is hoped that this research study will spark an interest in this area of research and also in the behavioural intentions of the malicious insiders/employees.

This study has contributed to the body of knowledge though a journal publication (See Appendix A). Another paper has also been submitted for journal publication and another one for a conference and both papers are currently under review.

The researcher acknowledges the lack of an extensive critical review of the existing literature on human psychology. Current literature in this context is very social science-based. However, the researcher's limited skill in this dimension did not provide sufficient basis for a critical review and, thus, the researcher limited the literature review to the works of the most influential theorists in the domain.

10.11. Summary

The TPB, the KAB theory and DT helped to conceptualise the factors that impact on employee behaviours. order to understand how behaviours are manifested in the information security context, the factors which play an effective role in information security, behavioural studies and psychology were collected from a review of the relevant literature, after which the initial framework was developed. This framework was also reviewed by a total of nine security experts

The value of this study may be determined by the impact it had on the information security compliance at CEF. It increased the levels of awareness of employees, thus reducing the risk of costly, naïve mistakes. This in turn improved the success of the organisation as it reduced the downtime caused by virus attacks and other information security incidences. Overall, information security awareness is crucial for SMEs because they usually do not sufficient resources to recover from such incidences.

This thesis comprised three research steps. The first step involved reviewing and evaluating literature relevant to the research topic while the second step involved designing, refining and evaluating frameworks through expert review and action research. The final step was to analyse the practicality of the frameworks and report on the findings.

LIST OF REFERENCES

Ajzen, I. (1991). The Theory of Planned Behaviour. *Organisational Behaviour and Human Decision Processes*, *50*(2), 179–211.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11-39). Springer Berlin Heidelberg.

Alavi, M., & Carlson, P. (1992). A review of MIS research and disciplinary development. *Journal of Management Information Systems*, *8*(4), 45-62.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & Security, 26(4), 276-289.

Alexander, J. C. (2014). Positivism, Presupposition and Current Controversies (Theoretical Logic in Sociology). Routledge.

Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. In *Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for* (pp. 352-358). IEEE.

Al Hogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behaviour*, *49*, 567–575.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security policy compliance: User acceptance perspective. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 3317-3326). IEEE.

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, *42*, 56–65.

Alnatheer, M., & Nelson, K. (2009). Proposed Framework for understanding information security culture and practices in the Saudi context.

Anderson,C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioural intentions. *MIS Quarterly*, *34*(1), 613–43.

Arage, T., Belanger, F., & Beshah, T. (2015). Influence of National Culture on Employees' Compliance with Information Systems Security (ISS) Policies: Towards ISS Culture in Ethiopian Companies.

Argyris, C., Putnam, R., & Smith, D. M. (1985). *Action science*. San Francisco: Jossey-Bass.

Ashenden, D. M. (2015). *Information security awareness: Improving current research and practice* (Doctoral dissertation, UCL (University College London)).

Babbie, E. (2007). The Practice of Social Research, Belmont, CA: Thomson Learning.

Bacik, S. (2008). *Building an effective information security policy architecture*. CRC Press.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organisational Behaviour and Human Decision Processes*, *50*(2), 248–87.

Banking Association of South Africa website. Retrieved May 13, 2017 from http://www.banking.org.za/what-we-do/sme/sme-enterprise

Baranowski, T., Cullen, K. W., Nicklas, T., Thompson, D., & Baranowski, J. (2003). Are current health behavioral change models helpful in guiding prevention of weight gain efforts?. *Obesity research*, *11*(S10), 23S-43S.

Baskerville, R. L. (1999). Investigating information systems with action research. *Communications of the AIS*, *2*(3es), 4.

Baskerville, R. L., & Wood-Harper, A. T. (2016). A critical perspective on action research as a method for information systems research. In *Enacting Research Methods in Information Systems: Volume 2* (pp. 169-190). Springer International Publishing.

Bates, L., Soole, D., & Watson, B. (2012). The effectiveness of traffic policing in reducing traffic crashes. In *Policing and security in practice* (pp. 90-109). Palgrave Macmillan UK.

Beccaria, C. (1963). On crimes and punishments (introduction by H. Paolucci, Trans.). New York: Macmillan.

Bem, D. J. (1972). Self-perception theory. *Advances in experimental social psychology*, *6*, 1-62.

BERR. (2008 April). *Information Security Breaches Survey: Technical Report*. Department for Business Enterprise and Regulatory Reform. URN 08/788.

Berlew, D. E., & Harrison, R. (1978). The Positive Power and Influence Program. *Plymouth, Mass.: Situation Management Systems*.

Bettinghaus, E. P. (1986). Health promotion and the knowledge-attitude-behavior continuum. *Preventive medicine*, *15*(5), 475-491.

Bhattacherjee, A., & Sanford, C. (2009). The intention–behaviour gap in technology usage: the moderating role of attitude strength. *Behaviour & Information Technology*, *28*(4), 389-401.

Bidmon, S. (2017). How does attachment style influence the brand attachment–brand trust and brand loyalty chain in adolescents?. *International Journal of Advertising*, *36*(1), 164-189.

Blaikie N. (2010). *Designing Social Research* , 2nd ed. Polity Press.

Blumstein, A., Cohen, J., & Nagin, D. (1978). *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates* (p. 431). Washington, DC: National Academy of Sciences.

Bobek, D. D., Hageman, A. M., & Kelliher, C. F. (2013). Analyzing the role of social norms in tax compliance behavior. *Journal of Business Ethics*, *115*(3), 451-468.

Boeckeler, M. C. (2004). *Overview of security issues facing computer users*. SANS Institute, InfoSec Reading Room.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151-164.

Breckler, S. J. (1984). Empirical validation of affect, behavior, and cognition as distinct components of attitude. *Journal of personality and social psychology*, *47*(6), 1191.

Brewer, D. (2013). *An Introduction to ISO/IEC 27001: 2013*. BSI British Standards Institution.

Brinkmann, S. (2014). *Interview* (pp. 1008-1010). Springer New York.

Brodie, C. (2008). *The importance of security awareness training*. SANS Institute, InfoSec Reading Room.

Brown, A. D. (1997). Narcissism, identity, and legitimacy. *Academy of management Review*, *22*(3), 643-686.

Brubaker, R. G., & Fowler, C. (1990). Encouraging College Males to Perform Testicular Self-Examination: Evaluation of a Persuasive Message Based on the Revised Theory of Reasoned Action1. *Journal of Applied Social Psychology*, *20*(17), 1411-1422.

Brunetti, L., Santoro, E., De Caro, F., Cavallo, P., Boccia, A., Capunzo, M., & Motta, O. (2015). Surveillance of nosocomial infections: a preliminary study on hand hygiene compliance of healthcare workers. *Journal of Preventive Medicine and Hygiene*, *47*(2).

Bucher, J., Donovan, C., Ohman-Strickland, P., & McCoy, J. (2015). Hand washing practices among emergency medical services providers. *Western Journal of Emergency Medicine*, *16*(5), 727.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190–209.

CERT. (2007). *E-Crime Survey*. Retrieved 10 February 2009, from Over-Confidence is Pervasive amongst Security Professionals: www.cert.org/archive/pdf/ecrimesummary07.pdf

CERT. (2010). *Cybersecurity Watch Survey*. Retrieved 10 June 2012, from http://www.cert.org/archive/pdf/ecrimesummary10.pdf.

Chapple. M. (2005). Four ways to measure security success. Risk Management Strategies. From http://www.techtarget.com/search/query?q=chapple

Chambliss, D. F., & Schutt, R. K. (2012). *Making sense of the social world: Methods of investigation*. Sage.

Chan, L., & Bishop, B. (2013). A moral basis for recycling: Extending the theory of planned behaviour. *Journal of Environmental Psychology*, *36*, 96-102.

Chau, D. H. P., Nachenberg, C., Wilhelm, J., Wright, A., & Faloutsos, C. (2011). Polonium: Tera-scale graph mining and inference for malware detection. In *Proceedings of the 2011 SIAM International Conference on Data Mining* (pp. 131-142). Society for Industrial and Applied Mathematics.

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior*, *38*, 220-228.

Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security*, (3), 13–19.

Chou, K. T. (2007). Biomedtech Island Project and Risk Governance. Paradigm conflicts within a hidden and delayed high-tech risk society. *Soziale Welt*, 123-143.

Cram, W. A., Proudfoot, J., & D'Arcy, J. (2017, January). Seeing the forest and the trees: A meta-analysis of information security policy compliance literature. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

CSO Magazine. (2010). US Secret Service. *Software Engineering Institute, CERT Program at Carnegie Mellon University and Deloitte*.

Collis, J., & Hussey, R. (2009). *Quantitative methods for business and management* (3rd ed.). New York: Palgrave Macmillan.

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days?. *Information Security Technical Report*, *14*(4), 186–196.

Cooke, R., Dahdah, M., Norman, P., & French, D. P. (2016). How well does the theory of planned behaviour predict alcohol consumption? A systematic review and meta-analysis. *Health psychology review*, *10*(2), 148-167.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behaviour, 28*(5), 1849–1858.

Cushman, F., & Morris, A. (2015). Habitual control of goal selection in humans. *Proceedings of the National Academy of Sciences*, *112*(45), 13817-13822.

Czellar, S. (2006). Self-presentational effects in the Implicit Association Test. *Journal of Consumer Psychology*, *16*(1), 92-100.

D'arcy, J., & Herath, T. (2011). A review and analysis of Deterrence Theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658.

Danchev, D. (2003). *Building and Implementing a successful information security policy.* Retrieved May 13, 2009 from www.windowsecurity.com.

Da Veiga, A., & Eloff. J. H. P. (2010). A framework and assessment instrument for Information Security Culture, *Computers & Security*, *29*(2), 196–207.

David, M., & Sutton, C. D. (2011). *Social research: An introduction*. Sage.

Davison, R. M., Martinsons, M. G., & Kock, N. (2004). Principles of canoncial action research. *Information Systems Journal, 14*, 65–86.

De Vaus, D. (2013). *Surveys in social research*. Routledge.

De Vos, A. S., Strydom, H., Fouché, C. B., & Delport, C. S. L. (2005*). Research at grass roots: For the social sciences and human service professions*. Pretoria: Van Schaik.

Della Porta, D., & Keating, M. (2008). How many approaches in the social sciences? An epistemological introduction.

Denzin, N. K., & Lincoln, Y. S. (2011). *The Sage handbook of qualitative research*. Sage.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, *19*(4), 391-412.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3), 189-198.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security*, *26*(1), 36-43.

Dubé, L., & Paré, G. (2003). Rigor in information systems positivist case research: current practices, trends, and recommendations. *MIS quarterly*, 597-636.

Duchon, D., & Burns, M. (2008). Organizational narcissism. *Organizational Dynamics,* 37(4), 354–364.

Du Plessis, L., & Von Solms, R. (2002). Information security awareness: Baseline education and certification. *Information Technology on the Move*, 101.

Dupuis, M. J., Crossler, R. E., & Endicott-Popovsky, B. (2016, January). Measuring the human factor in information security and privacy. In *2016 49th Hawaii International Conference on System Sciences (HICSS),* 3676-3685. IEEE.

Durcikova, A., & Jennex, M. (2017). Introduction to Confidentiality, Integrity, and Availability of Knowledge and Data Minitrack.

Elden, M., & Chisholm, R. F. (1993). Emerging varieties of action research: Introduction to the Special Issue. *Human Relations, 46*(2), 121–142.

Elky, S. (2006). An Introduction to Information System Risk Management. *SANS Institute InfoSec Reading Room.*

Elliott, J. (2011). *Reconstructing teacher education* (Vol. 221). Routledge.

Ellis, T. J., & Levy, Y. (2012). Data sources for scholarly research: Towards a guide for novice researchers. In *Proceedings of Informing Science and IT Education Conference*.

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies: A case study. *Information Security Technical Report*, *14*(4), 223–229.

ENISA (2007). Current practice and the measurement of success. Retrieved February 3, 2015 from: http://bookshop.europa.eu/lv/information-security-awareness-initiatives

Etsebeth, V. (2006). Information Security Policies-The Legal Risk of Uninformed Personnel. In *ISSA*, 1-10.

Evans, J. S. B. (2013). *The Psychology of Deductive Reasoning (Psychology Revivals)*. Psychology Press.

F-Secure (2015). 2017 State Of Cyber Security Report. From https://www.f-secure.com/en/welcome

Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information sciences*, *256*, 57-73.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behaviour: An introduction to theory and research.* Massachusetts: Addison-Wesley.

Furnell, S. (2006). Malicious or misinformed? Exploring a contributor to the insider threat. *Computer Fraud & Security*, (9), 8–12.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27-35.

Furnell, S., & Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security*, (3), 12–15.

Furnell, S., & Thompson, K. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, (2), 5–10.

Flowerday, S., & Von Solms, R. (2005). Real-time information integrity = system integrity + data integrity + continuous assurances. *Computers & Security, 24*(8), 604–613.

Gallagher, S., & Sixsmith, A. (2014). Engaging IT undergraduates in non-IT content: Adopting an eLearning information system in the classroom. *Interactive Technology and Smart Education*, *11*(2), 99-111.

Gephart, R. (1999). Paradigms and research methods. In *Research methods forum.* 4(1), 11-25.

Godin, S. (2009). *Purple Cow, New Edition: Transform Your Business by Being Remarkable*. Penguin.

Goo, J., Yim, M. S., & Kim, D. J. (2014). A path to successful management of employee security compliance: An empirical study of information security climate. *Professional Communication*, IEEE Transactions on, *57*(4), 286–308.

Greig, A., Renaud, K., & Flowerday, S. (2015, October). An ethnographic study to assess the enactment of information security culture in a retail store. *Internet Security (WorldCIS), 2015 World Congress,* 61-66. IEEE.

Guba, E. G., & Lincoln, Y. S. (1981). *Effective evaluation: Improving the usefulness of evaluation results through responsive and naturalistic approaches*. Jossey-Bass.

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, *104*(2), 69-79.

Gundu, T., & Flowerday, S. V. (2012). The enemy within: A behavioural intention model and an information security awareness process. *Information Security for South Africa (ISSA), 2012,* 1-8. IEEE.

Hale, J. L., Householder, B. J., & Greene, K. (2002). Theory of reasoned action. In J. P. Dillard & M. Pfau (Eds.), The persuasion handbook: Developments in theory and practice (pp. 259–286). Thousand Oaks, CA: Sage.

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security, 3*(2), 154–165.

Hasan, R., Zawoad, S., Noor, S., Haque, M. M., & Burke, D. (2016). How secure is the healthcare network from insider attacks? an audit guideline for vulnerability analysis. *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual,* (1), 417-422). IEEE.

Helgeson, J., van der Linden, S., & Chabay, I. (2012). The role of knowledge, learning and mental models in public perceptions of climate change related risks. *Learning for Sustainability in Times of Accelerating Change; Wals, AJ, Corcoran, PN, Eds*, 329-346.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviours in organisations: Role of penalties, pressures and perceived effectiveness, *Decision Support System*, *47*(2), 154–165.

Hinson, G. (2006). Seven myths about information security metrics. *. Information Security for South Africa (ISSA), 2006,1-6. IEEE.*

Hirschheim, R. (1985). Information systems epistemology: An historical perspective. In E. Mumford, R. Hirschheim, G. Fitzgerald, & T. Wood-Harper (Eds.), Research methods in information systems (pp. 13-35). Amsterdam: North-Holland.

Hofstee, E. (2006). *Constructing a good dissertation*. Johannesburg: EPE.

Hogg, M. A., & Abrahams, D. (1988). *Social identifications: A social psychology of intergroup relations and group processes*. London and New York: Routledge.

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, *32*, 35–49.

Hovav, A. (2017). How Espoused Culture Influences Misuse Intention: A Micro-Institutional Theory Perspective. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM*, *54*(6), 54-60.

Hunter, B. (2000, April 14). *Information security: Raising awareness.* Retrieved April 06, 2009, from www.iwar.org.uk: http://www.iwar.org.uk/comsec/resources/canada-ia/inforsecawareness.htm

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1).

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the Theory of Planned Behaviour and the protection motivation theory. C*omputers & Security,* 31(1), 83–85.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79.

ISACA. (2009). An Introduction to the business model for information security. Retrieved February 3, 2010 from http://www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=48017

ISO/IEC 27002. (2013) Code of Practice for Information Security Management as a Base for Certification. *(AS ISO/IEC 27002: 2013), Standards Australia*.

Jayasingh, S., & Eze, U. C. (2015). An empirical analysis of consumer behavioural intention towards mobile coupons in malaysia. *International Journal of Business and Information*, *4*(2).

Jenkins, S., Goal, R., & Morrele, D. (2008). Computer-assisted instruction versus traditional lecture for medical student teaching of dermatology morphology: A randomized contol trial, *Journal of the American Academy of Dermatology*, *59*(2), 255−259.

Johnson, E. (2006). Security awareness: Switch to a better program. *Network Security*, (1), 15–18.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher, 33*(7), 14–26.

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of mixed methods research*, *1*(2), 112-133.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. T. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113–134.

Johnstone, M. (2001). *Security awareness training and privacy*. SANS Institute, Infosec Reading Room.

Joshi, Y., & Rahman, Z. (2015). Factors affecting green purchase behaviour and future research directions. *International Strategic Management Review*, *3*(1), 128-143.

Kabay, M. E. (2004). *What's important for information security: A managers guide*. Norwich UK: Norwich University.

Kabay, M.E. (2005). Improving information assurance education key to improving secure(ity) management. *Journal of Network and Systems Management*, *13*(3), 247–251.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & security*, *43*, 64-76.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International journal of information management*, *23*(2), 139-154.

Kautonen, T., Gelderen, M., & Fink, M. (2015). Robustness of the theory of planned behavior in predicting entrepreneurial intentions and actions. *Entrepreneurship Theory and Practice*, *39*(3), 655-674.

Kautonen, T., Van Gelderen, M., & Tornikoski, E. T. (2013). Predicting entrepreneurial behaviour: a test of the theory of planned behaviour. *Applied Economics*, *45*(6), 697-707.

Kelly, N., Harpel, T., Fontes, A., Walters, C., & Murphy, J. (2017). An Examination of Social Desirability Bias in Measures of College Students' Financial Behavior. *College Student Journal*, *51*(1), 115-128.

Kemmis, S., & Wilkinson, M. (1998). Participatory action research and the study of practice. *Action research in practice: Partnerships for social justice in education*, *1*, 21-36.

Klöckner, C. A., Matthies, E., & Hunecke, M. (2003). Problems of operationalizing habits and integrating habits in normative decision-making models. *Journal of Applied Social Psychology*, *33*(2), 396-417.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, *38*(2), 143-154.

Krefting, L. (1991). Rigor in qualitative research: The assessment of trustworthiness. *American journal of occupational therapy*, *45*(3), 214-222.

Kritzinger, E. (2009). *An information security retrieval and awareness model for industry* (Doctoral dissertation). ACM Digital Library.

Kruger, H. A., & Kearney, W.D. (2005). *Measuring information security awareness: A West Africa gold mining environment case study.* North West University.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296.

Kruger, H. A., & Kearney, W. D. (2008). Consensus ranking–An ICT security awareness case study. *Computers & Security*, *27*(7), 254-259.

Krumpal, I. (2013). Determinants of social desirability bias in sensitive surveys: a literature review. *Quality & Quantity*, *47*(4), 2025-2047.

Krutz, R. L., & Rusell, D. V. (2001). *The CISSP Prep Guide.* New York: John Wiley & Sons.

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, *37*(4), 372-386.

Kumar, S., & Phrommathed, P. (2005). *Research methodology* , 43-50. Springer US.

Langer, E. J. (1975). The illusion of control. *Journal of personality and social psychology*, *32*(2), 311.

Layton, T. P. (2016). *Information Security: Design, implementation, measurement, and compliance*. CRC Press.

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, *59*, 60–70.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–87.

Lee, S, Yoon, S.N., & Kim, J. (2008). The role of pluralistic ignorance in Internet abuse. *Journal of Computer Information Systems, 48*(3), 38-43.

Leedy, P. D., & Ormrod, J. E. (2001). Practical research: Planning and research.

Lichtman, M. (2013). Part III: Putting it all together. *Qualitative Research in Education*, 241–268.

Locke, J, (1909-14). Some thoughts concerning education. In C. W. Eliot (Ed.), *The Harvard Classics* (ch. XXXVII). New York: P.F. Collier & Son.

Ma, Q., Pearson, J. M., & Tadisina, S. (2005). An exploratory study into factors of service quality for application service providers. Information & Management, 42(8), 1067-1080.

Magklaras, G. B., & Furnell, S. M. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security*, *21*(1), 62-73.

Mason, J. 2002. Qualitative researching, 2nd, London: Sage.

McAfee. (2005). McAfee Labs Threats Report September 2005. From https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2005.pdf

McKelvey, B. (2009). From Fields to Science: Can Organization Studies make the Transition?. *Debating organization: Point-counterpoint in organization studies*, 47.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151-156.

McGuire, W. J. (1969). The nature of attitudes and attitude change. *The handbook of social psychology*, *3*(2), 136-314.

McLaughlin, M. D., & Gogan, J. (2017, January). InfoSec Research in Prominent IS Journals: Findings and Implications for the CIO and Board of Directors. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Merriam, S. B. (1998). *Qualitative Research and Case Study Applications in Education. Revised and Expanded from" Case Study Research in Education."* Jossey-Bass Publishers, 350 Sansome St, San Francisco, CA 94104.

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: A sourcebook. *Beverly Hills: Sage Publications*.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behaviour: A meta-analytic of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106–43.

Miller, K. (2005). *Communications theories: Perspectives, processes, and contexts.* New York: McGraw-Hill.

Mtebe, J. S., & Raisamo, R. (2014). Investigating students' behavioural intention to adopt and use mobile learning in higher education in East Africa. *International Journal of Education and Development using Information and Communication Technology*, *10*(3), 4.

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & security*, *48*, 267-280.

Mouton, J. (1996). *Understanding social research*. Van Schaik Publishers.

Muijs, D. (2011). *Doing quantitative research in education with SPSS*. London: Sage Publications.

Myers, M. D. (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, *21*(2), 241-242.

Myers, M. D. (2013). *Qualitative research in business and management*. Sage.

Neal, D. T., Wood, W., & Quinn, J. M. (2006). Habits—A repeat performance. *Current Directions in Psychological Science*, *15*(4), 198-202.

Newbould, M., & Furnell, S. (2009). Playing Safe: A prototype game for raising awareness of social engineering. *Australian Information Security Management Conference,* 23-30.

Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers & Security*, *53*, 132-142.

Nosworthy, J. D. (2000). Implementing information security in the 21st century: Do you have the balancing factors? *Computers & Security, 19*(2), 337–347.

Oates, B. J. (2006). New frontiers for information systems research: computer art as an information system. *European Journal of Information Systems*, *15*(6), 617-626.

Odoom, R., Agbemabiese, G. C., Anning-Dorson, T., & Mensah, P. (2017). Branding capabilities and SME performance in an emerging market–the moderating effect of brand regulations. *Marketing Intelligence & Planning*, *35*(4).

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behaviour and awareness. *Computers & Security*, *56*, 83–93.

Ormston, R., Spencer, L., Barnard, M., & Snape, D. (2014). The foundations of qualitative research. *Qualitative research practice. A guide for social science students and researchers*, 1-25.

Otero, A. R. (2015). An information security control assessment methodology for organisations' financial information. *International Journal of Accounting Information Systems*, *18*, 26–45.

Ouellette, J. A., & Wood, W. (1998). Habit and intention in everyday life: The multiple processes by which past behavior predicts future behavior. *Psychological bulletin*, *124*(1), 54.

Oxford English Dictionary. (2002). Oxford English Dictionary. The Library.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, *31*(5), 673-680.

Pahnila, S., Siponen, M., & Mahomood, A. (2007 January). Employees' behaviour towards IS security policy compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences*. 3–6. Los Alamitos, CA.

Park, E. H., Kim, J., & Park, Y. S. (2017). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security*, *65*, 64–76.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). *Human factors and information security: individual, culture and security environment.* Defence Science and Technology Organisation, Edinburgh (Australia), Command Control Communications and Intelligence Div.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, 42, 165-176.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security,* 66, 40-51.

Patton, M. Q. (1987). *How to use qualitative methods in evaluation* (No. 4). Sage.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS quarterly*, 115-143.

Payne, S. C. (2010). A guide to security metrics. *SANS Security Essentials GSEC Practical Assignment Version*, *1*.

Pechmann, C., Zhao, G., Goldberg, M., & Reibling E. T. (2003). What to convey in antismoking advertisements of adolescents: the use of protection motivation theory to identify effective message themes, *Journal of Marketing, 6*, 1–18.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45-77.

Peltier, T. R. (2005). Implementing an information security awareness program. *EDPACS*, *33*(1), 1–18.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioural science to mitigate cyber security risk. *Computers & Security, 31*(3), 597–611.

Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage. Harvard Business Review, 63(4), 147-152.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, *51*(5), 551-567.

Potrac, P., Jones, R., & Nelson, L. (2014). *Interpretivism*. 31-41. L. Nelson, R. Groom, & P. Potrac (Eds.). London: Routledge.

Power, R. (2002). CSI/FBI computer crime and security. *Computer Security Journal, 17*(1), 7–30.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly*, 757-778.

Punch, K. F. (2013). *Introduction to social research: Quantitative and qualitative approaches*. Sage.

PricewaterhouseCoopers (PwC) (2014). The Global State of Information Security Survey. Retrieved 3 July 2015, from http://www.pwc.com/gx/en/consulting-services/information-security-survey/pwc-gsiss-2014-key-findings-report.pdf

PricewaterhouseCoopers (PwC) (2015). The Global State of Information Security Survey. Retrieved 17 July 2016, from http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

Regenbrecht, H., Schubert, T., Botella, C., & Baños, R. (2017). Mixed Reality Experience Questionnaire (MREQ)-Reference.

Reynolds, G. S. (1975). *A primer of operant conditioning* (Rev ed). Glenview, IL: Scott Foresman.

Richardson, R. (2008). CSI Computer Crime And Security Survey. *Computer Security Institute*, *1*, 1-30.

Ricer, R. E., Filak, A. T., & Short, J. (2005). Does a high tech (computerized, animated, PowerPoint) presentation increase retention of material compared to

a low tech (black on clear overheads) presentation? *Journal of Teaching and Learning in Medicine*, *17*(2), 107−111.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, *52*(3), 596.

Robson, C. (2002). Real world research: a resource for social scientists and practitioner. *Adapting Open Innovation in ICT Ecosystem Dynamics References Real World Research: A Resource for Social Scientists and Practitioner*, 270.

Rogers, R.W. (1983). Cognitive and physiological processes in fear-based attitude change: A revised theory of protection motivation. In J. Cacioppo, & R. Petty, (Eds), *Social psychophysiology: a sourcebook* . 153–76. New York: Guilford Press.

Rossman, G. B., & Rallis, S. F. (2003). *Learning in the field: An introduction to qualitative research*. California: Sage Publications.

Rosemann, M., & Vessey, I. (2008). Toward improving the relevance of information systems research to practice: the role of applicability checks. *Mis Quarterly*, 1-22.

Russell, C. (2002). *Security awareness: Implementing an effective strategy*. SANS Institute, InfoSec Reading Room.

Ryan, J. J., & Ryan, D. J. (2006). Expected benefits of information security investments. *Computers & Security*, *25*(8), 579-588.

Safa, N. S., & Maple, C. (2016). Human errors in the information security realm: And how to fix them. *Computer Fraud & Security*, (9), 17–20.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organisations. *Computers in Human Behaviour*, *57*, 442–451.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70-82.

Sarkar, R. K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Reports 15*(15), 112–133.

Saunders, M. L., & Lewis, P. (2009). P. & Thornhill, A.(2009). *Research methods for business students*, *4*.

SC Magazine. (2010). November 2010 Issue Of SCMagazine UK. From https://www.scmagazineuk.com/issue/november/01/2010/2740.

Schaffers, H., Guzman, G., & Merz, C. (2008). *An action reaserch approach to rural living labs innovation.* 2 Universidad Carlos III de Madrid.

Schlienger, T., & Teufel, S. (2005). Tool supported management of information security culture. *In IFIP International Information Security Conference*. 65-77. Springer US.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world.* New Jersey: John Wiley & Sons.

Schneier, B. (2008). *Schneier on security*. New Jersey: John Wiley & Sons.

Schulze, H. (2016). Insider Threat Spotlight Report. From http://crowdresearchpartners.com/wp-content/uploads/2016/09/Insider-Threat-Report-2016.pdf

Schwabe, L., & Wolf, O. T. (2011). Stress-induced modulation of instrumental behavior: from goal-directed to habitual control of action. *Behavioural brain research*, *219*(2), 321-328.

Schwitzgebel, E., & Rust, J. (2014). The moral behavior of ethics professors: Relationships among self-reported behavior, expressed normative attitude, and directly observed behavior. *Philosophical Psychology*, *27*(3), 293-327.

Seale, C. (2004). *Researching society and culture*. Sage.

Shaw, E., Ruby, K., & Post, J. (1998). The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin*, *2*(98), 1–10.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92-100.

Sheeran, P. (2002). Intention—behavior relations: A conceptual and empirical review. *European review of social psychology*, *12*(1), 1-36.

Sheeran, P., Trafimow, D., & Armitage, C. J. (2003). Predicting behaviour from perceived behavioural control: Tests of the accuracy assumption of the theory of planned behaviour. *British Journal of Social Psychology*, *42*(3), 393-410.

Sheeran, P., & Orbell, S. (1998). Do intentions predict condom use? Metaanalysis and examination of six moderator variables. *British Journal of Social Psychology*, *37*(2), 231-250.

Sheeran, P., & Webb, T. L. (2016). The intention–behavior gap. *Social and Personality Psychology Compass*, *10*(9), 503-518.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical opinion Are employees putting your company at risk by not following information security policies? Communications of the ACM, 52(12), 145-147.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Skinner, B.F. (1965). *Science and human behaviour*. Columbus, OH: Free Press.

Smart, K. L., & Cappel, J. J. (2006). Students' perceptions of online learning: A comparative study. *Journal of Information Technology Education*, *5*, 201−202.

Solutions, V. E. (2014). Verizon 2014 data breach investigations report. *verizon. com*, 13-15.

Sookdawoor, O. (2005). *An investigation of information security policies and practices in Mauritius*. UNISA, Johannesburg.

Staats, A. W., & Staats, C. K. (1958). Attitudes established by classical conditioning. *The Journal of Abnormal and Social Psychology, 57*(1), 37–58.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviours. *Computers & Security*, *24*(2), 124–133.

Steele, S., & Wargo, C. (2007). An introduction to insider threat management. Information Systems Security, 16(1), 23-33.

Stephanou, A. T., & Dagada, R. (2006). *The impact of information security awareness training on information security behaviour: The case study for further research.* University of Witwatersrand, Johannesburg.

Straub, D., & Ang, S. (2011). Editor's comments: Rigor and relevance in IS research: Redefining the debate and a call for future research. *MIS quarterly*, iii-xi.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research* (Vol. 15). Newbury Park, CA: Sage.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems. N. I. S. T.

Susanto, H., & Chen, C. K. (2017). Information and Communication Emerging Technology: Making Sense of Healthcare Innovation. In *Internet of Things and Big Data Technologies for Next Generation Healthcare*. 229-250. Springer International Publishing.

Talaei-Khoei, A., Solvoll, T., Ray, P., & Parameshwaran, N. (2011). Maintaining awareness using policies; Enabling agents to identify relevance of information. *Journal of Computer and System Sciences*, *78*(1), 370–391.

Talbot, S., and Woodward, A. (2009). Improving an organisations' existing information technology policy to increase security. *Proceedings of the 7th Australian Information Security Management Conference*. 8, 120 - 128.

Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. Computers & Security, 43, 19-34.

Teddlie, C., & Tashakkori, A. (2009). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences*. Sage.

Terreblanche, M., Durrheim, K., & Painter, D. (2006). *Research in practice*. Cape Town: University of Cape Town Press.

Thomas, P.Y. (2010). *Towards developing a web-based blended learning Environment at the University of Botswana* (D.Ed thesis in Didactics) University of South Africa, Pretoria.

Thrul, J., Bühler, A., & Herth, F. J. (2014). Prevention of teenage smoking through negative information giving, a cluster randomized controlled trial. *Drugs: education, prevention and policy*, *21*(1), 35-42.

Trochim, W. M. (2006). Qualitative validity. *Research methods knowledge base*, 1-3.

Urquhart, C., & Fernandez, W. (2013). Using grounded theory method in information systems: the researcher as blank slate and other myths. *Journal of Information Technology*, *28*(3), 224-236.

Van den Driest, F., & Weed, K. (2014). The ultimate marketing machine. *Harvard Business Review*, *92*, 54-63.

Van Loenen, J. (2015). Information security awareness. *Research World*, *2015*(54), 53-53.

Van Nes, N. (2010). Understanding replacement behaviour and exploring design solutions. *Longer lasting products: alternatives to the throwaway society*, 107-131.

Van Niekerk, J., & Von Solms, R. (2004). Organisational learning models for information security*. Information Security for South Africa (ISSA), 2004, 1-8. IEEE.*

Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*, 476–86.

Verplanken, B., Aarts, H., Knippenberg, A., & Moonen, A. (1998). Habit versus planned behaviour: A field experiment. *British journal of social psychology*, *37*(1), 111-128.

Von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, *20*(3), 215-218.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*, 371–376.

Voss, B. D. (2001). *The ultimate defense of depth: Security awareness in your company.* SANS Institute, InfoSec Reading Room.

Vreede, G.J. (1995) Facilitating Organizational Change" Doctoral Dissertation, Delft University of Technology, The Netherlands

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *24*, 191–198.

Walsham, G. (1995). The Emergence of Interpretivism in IS Research, *Information Systems Research* 6(4): 376–394.

Weaver, G., Furr, A., & Norton, R. (2016). Deception of Phishing: Studying the Techniques of Social Engineering by Analyzing Modern-day Phishing Attacks on Universities.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security, 44*, 1–15.

William, H. (2002). *Methods and techniques of implementing a security awareness program.* SANS Institute, InfoSec Reading Room.

Williams, P. A. (2008). In a 'trusting' environment, everyone is responsible for information security. *Information Security Technical Report*, *13*(4), 207–215.

Williams, P. A. (2009). What does security culture look like for small organisations?. *Proceedings of the 7th Australian Information Security Management Conference.* 48–54. Perth, Australia.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems*, *15*(4), 403-414.

Wilson, M., & Hash, J. (2003). *Building an Infomation technology security awareness and training program.* National Institute of Standards and Technology.

Wilson, S. (2008). *Research is ceremony: Indigenous research methods*.

Willson, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through situational crime prevention. *Communications of the ACM*, *52*.

Wood, B. (2000). An insider threat model for adversary simulation. *SRI International, Research on Mitigating the Insider Threat to Information Systems*, *2*, 1–3.

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A protection motivation theory approach to home wireless security. In D. Avison, D. Galletta & J. I. DeGross (Eds), *Proceedings of the 26th International Conference on Information Systems*. 367–380. Las Vegas, December 11–14.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behaviour*, *24*(6), 2799–2816.

Wright, D., Gutwirth, S., Friedewald, M., De Hert, P., Langheinrich, M., & Moscibroda, A. (2009). Privacy, trust and policy-making: Challenges and responses. Computer Law & Security Report, 25(1), 69-83.

Yildirim, E. (2016). The Importance of Information Security Awareness for the Success of Business Enterprises. In *Advances in Human Factors in Cybersecurity.* 211-222. Springer International Publishing.

Zviran, M., & Haga, W. J. (1999). Password security: an empirical study. *Journal of Management Information Systems*, *15*(4), 161-185.

APPENDICES

Appendix A

This appendix contains copies of publications from this research study.

1. Publication

IGNORANCE TO AWARENESS: TOWARDS AN INFORMATION SECURITY AWARENESS PROCESS

T. Gundu* and S.V. Flowerday**

** Department Information Systems, University of Fort Hare, 50 Church Street, East London, South Africa, 5201 E-mail: tapgun@gmail.com*
*** Department Information Systems, University of Fort Hare, 50 Church Street, East London, South Africa, 5201 E-mail: sflowerday@ufh.ac.za*

Abstract: With most employees in small and medium enterprise (SME) engineering firms now having access to their own personal workstations, the need for information security management to safeguard against loss/alteration or theft of the firms' important information has increased. These SMEs tend to be more concerned with vulnerabilities from external threats, although industry research suggests that a substantial proportion of security incidents originate from insiders within the firm. Hence, physical preventative measures such as antivirus software and firewalls are proving to solve only part of the problem as the employees using them lack adequate information security knowledge. This tends to expose a firm to risks and costly mistakes made by naïve/uninformed employees. This paper presents an information security awareness process that seeks to cultivate positive security behaviours using a behavioural intention model based on the Theory of Reasoned Action, the Protection Motivation Theory and the Behaviourism Theory. The process and model have been refined, tested through action research at an SME engineering firm in South Africa, and the findings are presented and discussed in this paper.

Keywords: Information Security Awareness, Security Behaviour, Information Security Training.

1. INTRODUCTION

SMEs, especially those in the engineering sector, are continually investing significantly in their overall Information and Communication Technologies (ICTs) making Information Security a major concern for the safeguarding of their information assets [10]; [15].

Most of these SMEs have information security policies that present rules to be adhered to [19]. These rules provide a solid foundation for the development and implementation of secure practices within the firms. However, the existence of these formal security policies does not necessarily mean that employees will adhere to the rules [10]. Subsequently, employees need to be aware of the security practices prescribed in the firm's policy.

Information security awareness and training are frequently used for raising awareness of employees and promoting appropriate information security behaviour. This ensures their employees realise the importance of security and the adverse consequences of information security failure plus that there is the potential for people to deliberately or accidentally steal, damage, or misuse data stored within a firm's information systems and throughout the organisation [20]; [45].

Engineering firms rely heavily on digital information stored on networked servers. This information includes patented and unpatented private and confidential designs, plus drawings and client information that are prone to security threats. Engineering SMEs tend to ignore the risk of the uninformed employee and are more concerned with vulnerabilities from external threats; however, industry research suggests that the uninformed employee, by not behaving securely, may expose the firm to serious security risks, for example: data corruption, deletion, and even commercial espionage [1]; [5]; [6]; [22]; [33].

Insider risk can result from two sources: intentional and unintentional behaviour [45]. This paper focuses on unintentional naïve mistakes although intentional dangerous tinkering by disgruntled employees is also a significant threat. Unintentionally uninformed employees (insiders) may expose a firm's information assets to risk by making naïve mistakes, visiting malware infested websites, responding to phishing emails, using weak passwords, storing their login information in unsecured locations, or giving out sensitive information over the phone when exposed to social engineering techniques. Unintentional mistakes by the employee is not an attempt to discredit the firm or make a profit by selling confidential data, but rather as a result of inadequate employee training about information security, that is their lack of security awareness and the consequences of their actions. This weakness can never be totally eliminated, but a well-structured security awareness campaign helps to reduce the risk to acceptable levels [19]; [22].

SME Engineering firms have high levels of trust in their employees not to compromise security; hence, they believe information security awareness is not an issue for them [42]. Ironically, it is more important for SMEs compared to larger firms as employees often have multiple roles and thus have access to a variety of financial, organisational, customer and employee information. Furthermore, there is less segregation of duties in SME engineering firms, thus less control over access to information. Whilst exposed to many of the same threats and vulnerabilities as large organisations,

Based on "The Enemy Within: A behavioural intention model and an information security awareness process", by Tapiwa Gundu and Stephen V Flowerday which appeared in the Proceedings of Information Security South African (ISSA) 2012, Johannesburg, 15 to 17 August 2012.

SMEs do not have access to the same level of resources [42]; this makes their risk even higher.

The purpose of this paper is to present, refine and validate a process that can be followed by SMEs to ensure that their employees are information security aware. This process is mainly based on a behavioural intention model to be presented in section 3.2 and Kruger and Kearney's [21] information security measuring concepts.

The behavioural intention model bases its argument on three principal theories: the Theory of Reasoned Action (TRA) [3], the Protection Motivation Theory (PMT) [28] and the Behaviourism Theory (BT) [47]. Previous works have used research frameworks that integrated TRA, PMT and BT with other theories (even if unconsciously) [10]; [13]; [30]. According to Anderson and Agarwal's [27] review of literature in this area, no prior information security research has used all three theories in a single information security study. Although research has been carried out in the area of information security awareness, there is a lack of literature on the effectiveness of information security awareness methods on the basis of psychological theories as well as a lack of description of the underlying theory of these methods. Psychology is the science of the mind and behaviour. Social psychology has been used for many years for research in the area of education, learning and human behaviour [29].

Action Research was conducted at a civil engineering firm to refine and validate the process. Elden and Chisholm [44] note that action research is change oriented, seeking to introduce changes with positive social values, the key focus of the practice being on a problem and its solution.

The remainder of the paper is organised as follows: first, the information security awareness process is presented, then follows the behavioural intentional model; thirdly, the method for measuring information security is discussed; followed by the analysis and results; finally, the paper concludes by discussing its findings.

2. THE INFORMATION SECURITY AWARENESS PROCESS

Information security theories posit that in order for security efforts to be effective, firms must ensure that employees are part of the security effort [4]; [32]; [34]; [38]; [45].

This section discusses the proposed information security awareness process in the form of a flowchart. Figure 1 shows the proposed information security awareness process for SME engineering firms. The flowchart has four processes (P1, P2, P3 and P4) and three checks (C1, C2 and C3). When planning an information security awareness program, the first step should be to check the existence of an up-to-date Information Security Policy (C1 and C2); however, the firm where the action research was conducted had a sound and up-to-date policy that accurately reflected its overall posture towards information security. The step of drafting or updating an Information Security Policy (P1 and P2) was not carried out and is beyond the scope of this study.

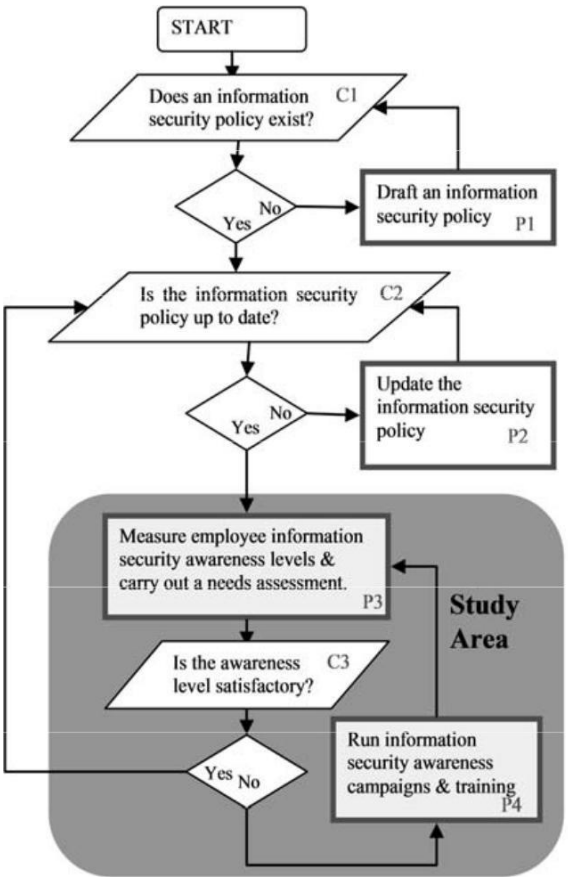


Figure 1: Information security awareness process

The next step is to measure employees' current level of information security understanding (P3) so as to identify any knowledge gaps. During the action research, this needs assessment process highlighted the firm's awareness and training requirements. For example, in the first iteration of the action research, the measurement revealed that employees had an inadequate understanding of password creation, safe Internet usage, virus and firewall understanding, thus highlighting some topics for awareness training. These results also justified to the firm's management the need to allocate resources towards information security awareness and training. The method for measuring employee awareness levels was adapted from Kruger and Kearney's [21] previous research; the details of this method will follow in section 4.

The next step would then be to verify if the current level of information security awareness is at an acceptable level (C3). When conducting the action research, it was found that the level of information security awareness during the first iteration was unsatisfactory and exposed the need for information security awareness campaigns and training. If the levels are unsatisfactory, awareness

campaigns and training sessions should be conducted. During the action research, an e-learning based awareness campaign/training was conducted (P4). Its implementation and maintenance is discussed in detail in section 4. The awareness level was measured again after the awareness campaign and results showed that the knowledge gap was closing, but the results were not yet satisfactory according to the scales used (these will be discussed in the data analysis section). The process was then run again for a second and third iteration. The results of the third iteration were satisfactory and the process was stopped.

3. INFORMATION SECURITY AWARENESS CAMPAIGN AND TRAINING (P4)

Awareness from a different perspective: "It is believed that about 200 years ago people did not know about the germ theory; they did not know that they should wash their hands and boil surgical tools to limit the spread of disease and infection. Even though people know these things today, do they always wash their hands before eating, or even after doing something icky?" [39].

Unfortunately, not everyone does so even when they know better. This highlights that the real challenge is not just to teach people, but also to help them change their behaviour. Security knowledge cannot help much if employees do not act on it; hence, this section provides guidelines for implementing and maintaining comprehensive e-learning information security awareness and training campaigns.

Security awareness and training assists in tempering the attitude that security policy is restrictive and interferes with an employee's ability to do his/her work. The better the employee's understanding of information security issues, the more they understand the importance of security and the ways in which security protects them and enables them to do their work in a safer and more effective environment [19].

Information security campaigns are divided into awareness and training. Awareness aims to raise the collective knowledge of information security and its controls, while training aims at facilitating a more in-depth level of employee information security understanding. An effective information security awareness and training programme seeks to explain proper rules of behaviour when using the firm's computer/information systems. The programme communicates information security policies and procedures that need to be followed. Additionally, the campaign imposes sanctions when noncompliance occurs [10].

The BERR 2008 survey [2] suggests that the majority of firms rely upon written materials for training in one form or another. However, simply developing and circulating a policy will not be sufficient to foster appropriate understanding and behaviour. Most companies use the traditional classroom style for awareness and training. However, this study seeks to apply the now widely used tried and tested e-learning concept to information security awareness and training. Jenkins et al [16] and Ricer et al [26] report that there is no significant difference between people who learn using a computer or the traditional classroom style in the short or long-term retention of knowledge.

Additionally this section introduces the behavioural intention model. This model attempts to explain how employee information security awareness knowledge can affect behavioural intentions (towards policy compliance and positive security culture) . Behaviourists believe that employees are born with limited innate reflexes (stimulus-response units that do not need to be learnt) and that all of an employee's complex behaviours are as a result of learning through interaction with the environment [47]. Thus, belief in information security awareness and training should help mould information security behaviours. The information security awareness campaigns and training in P4 on the Information Awareness Process (Figure 1) are based on a behavioural intention model to be explained next.

3.1 Theoretical background of the behavioural intention model

Based on the problems presented in the preceding sections, this section serves to propose, explain and relate the Theory of Reasoned Action (TRA), the Protection Motivation Theory (PMT) and the Behaviourism Theory (BT) to the behavioural intention model.

3.1.1 Theory of Reasoned Action

TRA framework specifically evaluates the relative importance of two incentive components: (1) attitude (2) subjective norm. It suggests that a person's Behavioural Intention (BI) depends on the person's Attitude (A) about the behaviour and Subjective Norms (SN) i.e. (BI = A + SN). Attitude towards behaviour is defined as the individual's positive or negative feelings about performing certain actions. Subjective norm is defined as an individual's perception of whether people important to the individual think the behaviour should be performed. As a general rule, the more favourable the attitude and the subjective norm, the greater the perceived control and therefore the stronger the employee's intention to perform the behaviour in question [7]; [17]; [23]; [29].

The Theory of Reasoned Action helps to explain how the employee's attitude towards security and perceived corporate expectation affects the employee's behaviour towards information security. Consequently, the employee's attitude and perceived expectations influence the employee's behavioural intention.

The employee's attitude is affected by cultural, dispositional and knowledge influences. Cultural influences are associated with the employee's background. Dispositional influences are associated with the employee's usual way of doing things. Knowledge influences are associated with the level of knowledge of the subject in question. The employee's attitude can therefore be moulded by information security awareness campaigns and training. The subjective norm is what the employee perceives the firm requires of him/her and perception of how peers would behave in similar scenarios [9]; [13]; [30]. Corporate expectations can therefore be communicated to employees via information security and training sessions. In summary, information security awareness campaigns will help change employee attitudes towards information security and will aid in communicating the firm's expectations to its employees.

3.1.2 Protection Motivation Theory

Protection Motivation Theory (PMT) was developed by Rogers (1983). It was developed from the expectancy value theories and the cognitive processing theories, its aim being to assist and clarify fear appeals. PMT has been noted as one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions [27]. Information security awareness and training instil knowledge in the employees and assists in motivating protection. In essence, protection motivation emanates from both the threat appraisal and the coping appraisal. Threat appraisal describes an individual's assessment of the level of danger posed by a threatening event [28]; [40]. It is composed of perceived vulnerability and perceived severity.

Threat appraisal:

1. Perceived vulnerability i.e. an employee's assessment of the probability of threatening events. In this study it refers to threats resulting from noncompliance with the firm's information security policy (ISP).
2. Perceived severity i.e. the severity of the consequences of the event. In this instance, imminent threats to the firm's information security may arise from noncompliance with the firm's ISP.

The coping appraisal aspect of PMT refers to the employee's assessment of his or her ability to cope with and avoid the potential loss or damage arising from the threat [40]. Coping appraisals are made up of self-efficacy, response efficacy and response cost.

Coping appraisal:

1. Self-efficacy: this factor emphasizes the employee's ability or judgment regarding his or her capabilities to cope with or perform the recommended behaviour. In the context of this paper, it refers to the sorts of skills and measures needed to protect the firm's information assets [11]; [30]; [40].
2. Response efficacy: this factor relates to the belief about the perceived benefits of the action taken by the individual [28]. Here, it refers to compliance with the information security policy as being an effective mechanism for detecting a threat to the firm's information assets.
3. Response cost: this factor emphasizes the perceived opportunity costs in terms of monetary, time and effort expended in adopting the recommended behaviour, in this instance the cost of complying with the ISP. Previous research has used PMT and found it useful in predicting behaviours related to an individual's computer security behaviour both at home and in the work situation [9]; [27], as well as Information Security Policy (ISP) compliance [10]; [30].

3.1.3 The Behaviourism Theory (BT)

Watson coined the term "*behaviourism [47]*." Critical of Wundt's emphasis on internal states, Watson urged psychology to focus on obvious measureable behaviours [47]. Watson believed that theorising thoughts, intentions or other subjective experiences was unscientific [47]. Behaviourism as a theory was primarily developed by Skinner [47]. According to Skinner [47] it loosely encompasses the work of other behavioual researchers like Thorndike, Tolman, Guthrie and Hull.

These investigators had similar underlying assumptions on the processes of learning. These basic assumptions are summarised as follows: First, learning is manifested by a change in behaviour. Second, the environment shapes behaviour. And third, the principles of contiguity (how close in time two events must be for a bond to be formed) and reinforcement (any means of increasing the likelihood that an event will be repeated) are central to explaining the learning process. For Behaviourism, learning is the acquisition of new behaviour through conditioning.

There are two types of possible conditioning:

1. Classical conditioning: where the behaviour becomes a reflex response to stimulus as in the case of Pavlov's Dogs. Pavlov was interested in studying reflexes when he saw that the dogs drooled without the proper stimulus. Although no food was in sight, the dogs still salivated. It turned out that the dogs were reacting to lab coats. Every time the dogs were served food, the person who served the food was wearing a lab coat [49]. Therefore, the dogs reacted as if food was on its way whenever they saw a lab coat. In a series of experiments, Pavlov then tried to figure out how these phenomena were linked. For example, he struck a bell when the dogs were fed. If the bell was sounded in close association with their meal, the dogs learned to

associate the sound of the bell with food. After a while, at the mere sound of the bell, they responded by salivating. Pavlov's work laid the foundation for many other psychologists including Watson's ideas. Watson and Pavlov shared both a disdain for "mentalistic" concepts (such as consciousness) and a belief that the basic laws of learning were the same for all animals whether dogs or humans [49].

2. Operant conditioning highlights reinforcement of behaviour by a reward or punishment. The theory of operant conditioning was developed by Skinner [47] and is known as Radical Behaviourism. According to Reynold [48] the word 'operant' refers to the way in which behaviour 'operates on the environment'. Briefly, a behaviour may result either in reinforcement, which increases the likelihood of the behaviour recurring, or punishment, which decreases the likelihood of the behaviour recurring. It is important to note that, punishment is not considered to be applicable if it does not result in the reduction of the behaviour, and so the terms punishment and reinforcement are determined as a result of the actions. Within this framework, behaviourists are particularly interested in measurable changes in behaviour [48]. In operant conditioning we learn to associate a response (our behaviour) and its consequence and thus to repeat acts followed by good results and avoid acts followed by bad results [48].

3.1.4 The Behavioural Intention Model

Following the preceding discussion, it can be observed that the TRA, PMT or the BT can effect desirable behavioural intention. However, the behavioural intention model in Figure 2 attempts to encourage better behavioural intentions by combining the three theories into one model. Discussions on the behavioural intention model are explained in this section.

Subjective norms have a positive effect on information security policy (ISP) compliance behavioural intention. TRA indicates that individuals' attitudes impact on behavioural intentions [24]. To that end, a positive attitude toward ISP compliance bodes well for good behavioural intention. Conversely, negative attitudes will diminish an individual's ISP compliance and good behavioural intention. Thus, individuals with positive beliefs and values about their firm's ISP might display favourable tendencies towards complying with such rules, requirements and guidelines [10]; [13].

Attitude toward Information Security Policy (ISP) compliance will have a positive effect on ISP compliance behavioural intention. With respect to ISP, it is to be expected that individuals with high information security capabilities and competence will appreciate the need to

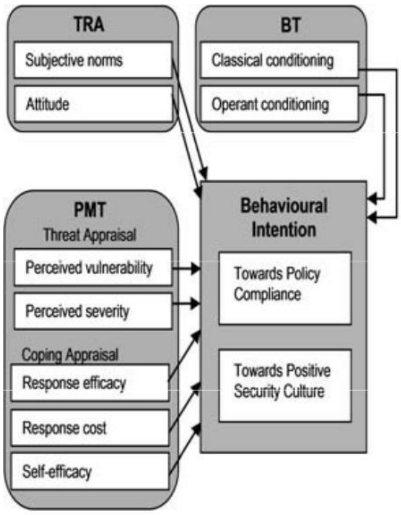


Figure 2: Behavioural intention model

follow organisational ISPs, and such individuals may be better placed to realise the threats of noncompliance [43]. Self-efficacy will have a positive effect on ISP compliance behavioural intention. According to Pahnila et al [30], response costs may include monetary expense, timing inconveniences, embarrassment or other negative consequences, which result from an individual's behaviour. Employees are reluctant to follow or adopt recommended responses if they perceive that a considerable amount of resources i.e. time, effort, and money will be used in pursuit of a low rewarding goal [8]; [9]. Conversely, if small amounts of resources are required in implementing a measure, it may be adopted [36]; [41]. Reducing the Response Cost tends to increase the likelihood of an individual performing a recommended behaviour [40]. Past studies have confirmed that Response Costs are negatively related to intention to use security measures [9]; [41].

Response Cost will have a negative effect on ISP compliance behavioural intention because usually employees believe information security measures are difficult and lengthy.

When an individual possesses requisite knowledge about the effectiveness of a recommended coping mechanism in providing protection from a threat or danger, the individual is more likely to adopt an adaptive behaviour [9]; [28]; [40]. If an individual has doubts regarding the effectiveness of a measure, he or she may not readily accept it [18]. Accordingly, individuals who believe that their organisation's ISP has guidelines and coping mechanisms to avert threats and dangers in their context, they are more likely to develop an intention to adopt it [10].

Response efficacy will have a positive effect on ISP compliance behavioural intention. In general, when employees perceive a threat, they often adjust their behaviour in response to the level of risk and determine if they are willing to accept the risk or not [8]; [41]. Thus,

an individual's perceived severity tends to be positively linked to their intentions to follow protective actions [36]. If an individual perceives a threat to his or her firm's Information Systems (IS) assets, such an individual will more than likely follow guidelines and requirements laid out in their ISP [13]; [30].

Perceived severity will have a positive effect on ISP compliance behavioural intention with respect to safe computing in the firm; however, individuals who consider themselves immune to security threats are more likely to ignore security measures at work [10]; [13]; [30]. It is reasonable to expect that an individual who perceives high risk to their firm's information system resource will be more likely to adopt protective behaviours.

Therefore, perceived vulnerability will have a positive effect on Information Security Policy (ISP) compliance behavioural intention because employees will be made aware of the vulnerability of the firms' information assets.

3.1.5 Information Dissemination Method (E-Learning)

When information security campaign material based on the needs assessment has been compiled, there is a need to choose a method for communicating the information to the employees. During the action research in this study, an e-learning method was used instead of the conventional classroom style because it provided a configurable infrastructure that integrated learning material, policies, and services into a single solution which quickly, effectively and economically created and delivered awareness and training content. E-Learning allows employees to train at their own convenience and learn at their own pace. It has also proved to be cheaper than bringing everyone together, in terms of time and money. This section therefore seeks to explain how e-learning can be used as a tool for communicating and testing information security awareness training.

E-learning has grown considerably over the past several years as technology has been integrated into education and training. E-learning may be defined as instruction delivered electronically via the Internet, Intranets, or multimedia platforms such as CD-ROM or DVD [35]. The literature review highlighted that research work on e-learning as a tool for information security awareness and training is still in its infancy and that no such tool has been used to date in SMEs.
The e-learning awareness and training program for this study was designed and developed by the researcher with assistance from a multimedia designer and a Web page developer using Macromedia Flash, Macromedia Dream Weaver, PDF, PowerPoint, Access, Gold Wave, and Photoshop software in order to present the program material in a visual and auditory format. This was presented in the form of a website containing information identified by the needs assessment and most relevant recent information security topics. Since information security is a diverse area with many topics, the importance of each topic varies from one firm to another depending on the nature of the risks faced so there is no universal information security awareness training. The training/awareness and testing could be completed in 1-3 hours depending on the speed at which the employee worked. The website for training and awareness was constructed as follows:

> **Home Page:** provides an introduction to information security and the motivation behind the training/ awareness campaign. Employees need to be motivated as to why information security is important. The home page then links to the awareness pages.
>
> **The Awareness/Training Pages:** supply information on topical issues and examples of breaches. These pages contain all the information about information security required by employees.
>
> **The Test Page:** was used as the data collection tool for acquiring data from the employees; this was used to measure their information security awareness levels.
> All the pages had attractive information security pictures/video clips/jokes in an effort to create a more relaxed e-learning environment.
> The employees participating in the study received an email with instructions on how to use the awareness and training material including a link to the awareness and training website.

E-Learning is a broad term and this paper wishes to stimulate the development of E-Awareness initiatives.

4. MEASURING INFORMATION SECURITY AWARENESS LEVELS (P3)

After the security awareness campaign was launched, it was important to measure its success and draw conclusions from the measured results. Measurement provides evidence of the campaign's effectiveness and reveals where knowledge gaps still exist. Measurements were not limited to a verification of whether the message was received by the target audience, but detected the effectiveness of the message, method and behavioural change.

According to a survey by Richardson [31], 32% do not measure information security awareness in their firms, because there are no commonly agreed and understood standard measurements for the effectiveness of information security awareness campaigns and training. Two distinctive challenges are identified when

developing a measuring tool and performing the actual measurements. These challenges are "what to measure" and "how to measure it" [12]; [21].

What to measure:

Kruger and Kearney [21] identified three components to be measured, namely what the employee knows (Knowledge), how they feel about the topic (Attitude), and what they do (Behaviour).

The attitude of employees towards information security is important because unless they believe that information security is important, they are unlikely to work securely, irrespective of how much they know about security requirements. Knowledge is important because even if an employee believes security is important, he or she cannot convert that intention into action without the necessary knowledge and understanding. Finally, no matter what employees believe or know about information security, they will not have a positive impact on security unless they behave in a secure fashion. Figure 3 below shows how enhanced security is achieved by correlating attitude, knowledge and behaviour.

Figure 3: Enhanced Security

How to measure:

Measuring such intangibles as Attitudes, Knowledge and Behaviour is difficult. The action research made use of multiple data collection techniques such as assessment tests, online surveys, participant observation, informal interviews and document surveys for gathering data. However, only the results from online assessment tests were used to calculate security awareness levels; information gathered using the other techniques was only used for needs assessments.

Online Survey and Assessment Tests enable identification of broad trends [14]. An agreement scale was used to allow employees to indicate degrees of agreement with statements about information security.

The assessment test contained questions that seek to test for knowledge, attitude and behaviour. The following are examples of the questions asked:

Example statement for test of knowledge:

Internet access to the firm's systems is a corporate resource and should be used for business purposes only.

1.True 2. False 3. Do not know

Example statement to test attitude:

Laptops are usually covered with existing insurance cover so there is no special need to include them in security policies.

1. True 2. False 3. Do not know

Example statement to test behaviour:

I am aware that one should never give one's password to somebody else; however, my work is of such a nature that I do give my password from time to time to a colleague (only to those I trust!).

1. True 2. False 3. Do not know

5. DATA ANALYSIS AND RESULTS

The engineering firm where the action research was conducted was established in 1997. It develops designs, plans, models and geotechnical surveys for the clients it consults. It has thirty two employees, four of whom have no access to the firm's computer resources. This left a sample size of twenty eight employees. The action research was conducted over a ten-month time period from February, 2011 to November, 2011.

In this action research, the researcher was not regarded as an objective, passive outsider. The firm's management expected him to be an active participator, helping to plan and deliver the training program and evaluate its results.
When the information security awareness of the employees was measured for the first time during the needs assessment, only 21% (6 employees) had sufficient levels of information security. Table 1 summarises the information security understanding of the employees per iteration.

Table 1: Employees information security awaremess understanding levels

	Needs assessment	Iteration 1	Iteration 2	Iteratio n 3
Employees understanding level	6 (21%)	18 (64%)	24 (86%)	27 (96%)

The number of employees with sufficient levels of information security understanding increased on the second iteration due to an increase in knowledge. The majority of employees had sufficient information security understanding after iteration 2 and 3.

All the employees were shown their test results and the overall group results during each iteration in order to

motivate those who had not performed well. However, the number of employees showing sufficient levels of

Figure 4: Awareness importance scale [21]

information security understanding is not a true reflection of a firm's overall information security awareness levels; hence Kruger and Kearney's [21] method of analysing data acquired through the measuring methods discussed in the preceding sections was used. This method involved weighting the three aspects being measured inas Figurefollows (Figure4. 4):

This weighting was verified with the Managing Director and the Human Resources Manager of the firm who agreed that behaviour was the most important measure followed by knowledge then lastly attitude. The results and importance weightings were processed in a spread sheet application and the output was finally presented in the form of graphs and awareness maps as comparable to Kruger and Kearney's study [21]. Table 2 below shows the scale used to interpret the level of awareness. Kruger and Kearney's scale was slightly modified to take into consideration recommendations by the firm's Managing Director. Figure 5 summarises the results categorised by Knowledge, Attitude and Behaviour.

Table 2: Awareness level measurements [21]

Awareness	Measurement (%)
Good	75
Average	60
Poor	30

The 78% awareness level in the 3rd iteration was satisfactory and there was no need for a fourth although it is advisable to run the process at least once a year as the skills and knowledge of the employees may become outdated.

It was possible to measure the effectiveness of the information security awareness training by using tools and methods outlined by Kruger and Kearney [21]. These enabled the firm to evaluate the extent to which awareness activities had impacted on behaviour, attitude, and knowledge and therefore, whether or not the initial training objectives had been met.

6. FINDINGS

Figure 5: Results summary

This study confirmed that having and implementing an information security policy does not automatically guarantee that all employees will understand their role in ensuring the security and safeguarding of information assets. It is therefore critical to design and align an information security awareness campaign to the information security policy's high-level goals, objectives and requirements.

The findings of the study support the Theory of Reasoned Action (TRA), the Protection Motivation Theory (PMT) and the Behaviourism Theory (BT). Awareness campaigns were aimed at communicating the firm's stance (subjective norm) on information security, threat appraisal, coping appraisal and in an effort to mould the employees' attitude towards positive behavioural intention. The results showed that an increase in knowledge made a positive change in attitude and behaviour.

However it was discovered that even though initially their security knowledge levels were very low, the employes had a positive attitude towards securing the firm's information assets; however, they did not have the skills and knowledge to behave in a secure manner confirming that the risk to which employees expose a firm is indeed due to unintentional naïve mistakes as was revealed by literature.

What is disappointing is that although knowledge increased dramatically during the iterations, the increase in attitude was marginal. This could be because employees have a certain attitude towards the firm and this attitude cannot be altered by information security awareness alone.

This study revealed that information security awareness programs require the largest portion of the information security budget which should be channelled to the design and implementation of an information security awareness campaign. This supports the findings of Voss [46]. It was revealed that the general costs of running information security awareness campaigns and training can be divided into direct and indirect costs.

Direct costs

Salary/incentives for the security awareness coordinator or team;
Training, including instructor fees and room rentals (in the case of classroom style training); and
Materials, such as slides, web designing, videos, posters, hand-outs and gadgets.

Indirect costs

Time spent by other employees or departments involved in promoting security awareness; and
Time spent by the target audience on courses and training.

Making use of e-learning campaign methods significantly reduced the costs of running the awareness campaign. Direct costs involved only the website designing cost, and the firm's in-house technician who was trained on updating and maintaining the website thereafter. Indirect costs reduced as employees took the courses during times they were not busy reducing the chance of productive time being lost.

While carrying out the action research the objectives were to refine and validate the process and change the behaviour of the employees at the particular SME. However, good information security behaviour cultivates an unpredicted information security culture. Hence it can be concluded that good information security awareness campaigns will ultimately result in a positive information security culture.

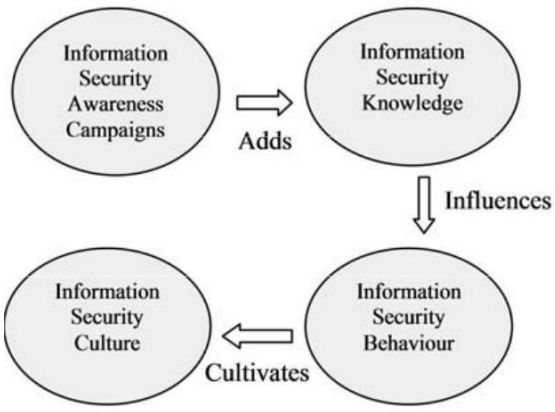


Figure 4: From information security awareness to information security culture

7. CONCLUSION

This paper was conceived against the backdrop of efforts made by SME firms to protect their information assets. This paper introduced an information security awareness process, which included behavioural intention models based on three persuasive theories i.e. Theory of Reasoned Action, Protection Motivation Theory and the Behaviourism Theory. The research findings showed that information security awareness levels greatly influence behavioural intentions.

The information security awareness process and behavioural intention was verified through expert review by initially nine information security experts. Additionally, it was refined and validated through action research. After the action research, three more experts reviewed the process and model against the results from the empirical work to further validate them. The information security process yielded positive information security behaviour from employees at the action research host firm during all iterations. The researcher is therefore almost certain that similar results would be achieved if the process and model were put into effect at SMEs with similar characteristics to the one where the study was conducted.

The authors recognise that although e-learning is not a novel idea, it is a relatively new aspect in the field of information security and has great potential to increase e-security awareness initiatives. This study area will become more apparent as e-learning within information security expands. Relating to that, this study has been able to promote e-learning as an effective type of learning compared to the traditional classroom style of learning.

This research study explored the risks exposed by the uninformed naïve employee to SME firms' information assets. However, the risks exposed by the malicious insider as well as the outsider still require further exploration.

8. REFERENCES

[1] R.Willson and M. Siponen. "Overcoming the insider: reducing employee computer crime through situational crime prevention", *Communications of the ACM*. Vol 52(9), September 2009. NY, USA.

[2] BERR. "Information Security Breaches Survey" – *Technical Report*. Department for Business Enterprise & Regulatory Reform. April 2008. URN 08/788.

[3] M. Fishbein, and I. Ajzen. *Belief, attitude, intention, and behaviour: An introduction to theory and research*, Massachusetts: Addison-Wesley, 1975.

[4] A. Da Veiga & J.H.P. Eloff. "A Framework and assessment instrument for Information Security Culture," *Computers & Security*, Vol 29(2), pp 196-207, March 2010.

[5] S. Furnell. "Malicious or misinformed? Exploring a contributor to the insider threat," *Computer Fraud & Security*. Vol 2006(9), pp 8-12, September 2006.

[6] S. Furnell and K. Thompson. "From culture to disobedience: Recognising the varying user acceptance of IT security" *Computer Fraud & Security*. Vol 2009 (2), pp 5-10, February 2009.

[7] J.L. Hale, B.J. Householder and K.L. Greene. The theory of reasoned action. In J. P. Dillard, and M. Pfau, *The persuasion handbook: Developments in theory and practice* (pp. 259 – 286). Califonia: Thousand Oaks, 2003.

[8] S. Milne, P. Sheeran and S. Orbell. "Prediction and intervention in health-related behaviour: a meta-analytic of protection motivation theory," *Journal of Applied Social Psychology*, Vol 30(1), pp 106- 43, 2000.

[9] Y. Lee and K.R. Larsen. "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software," *European Journal of Information Systems*, Vol 18(2), pp 177-87, 2009.

[10] T. Herath and H.R. Rao. "Encouraging information security behaviours in organisations: Role of penalties, pressures and perceived effectiveness," *Decision Support System*, Vol 47, pp 154 – 165, 2009.

[11] A. Bandura. "Social cognitive theory of self-regulation," *Organisational Behaviour and Human Decision Processes*, Vol 50, pp 248- 87, 1991.

[12] G. Hinson, "Seven myths about information security metrics," *originally published in ISSA Journal***,** July 2006, Available at: http://www.noticebored.com/html/metrics.html (Accesed Feb. 2010,)

[13] B. Bulgurcu, H. Cavusoglu and I. Benbasat. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* , Vol 34(3), pp 523-48, 2010.

[14] E. Hofstee. Literature Review. *In constructing a good dissertation.* Johannesburg: EPE, 2006.

[15] ISACA. (2009). An Introduction to the Business Model for Information Security. California. Available from: http://www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm &ContentID=48017 (Accessed 3 February 2010).

[16] S. Jenkins, R. Goal and D. Morrele. "Computer-assisted instruction versus traditional lecture for medical student teaching of dermatology morphology: A randomized control trial," *Journal of the American Academy of Dermatology*. Vol 59(2), pp 255−259, 2008.

[17] K. Miller. Communications theories: perspectives, processes, and contexts, New York: McGraw-Hill, 2005.

[18] P.A. Rippetoe and R.W. Rogers. "Effects of components of protection motivation theory on adaptive and maladaptive coping with a health threat," *Journal of Personnel Social Psychology*. Vol 52, pp 596-604, 1987.

[19] E. Johnson. "Security Awareness: Switch to a better program," *Network Security*. Vol 6, pp 15-18, 2006.

[20] M.E. Kabay. "Improving Information Assurance Education Key to Improving Secure(ity) Management." *Journal of Network and Systems Management*. Vol 13, pp 247-251, 2005.

[21] H.A. Kruger and W.D. Kearney. "A Prototype for assessing information security awareness," *Computers & Security*. Vol 25(4), pp 289 – 296, 2006.

[22] R.L. Krutz and D.V. Rusell. *The CISP Prep Guide*. New York: John Willey & Sons, 2001.

[23] K. Miller. *Communications theories: perspectives, processes, and contexts*. New York: McGraw-Hill, 2005.

[24] I. Ajzen. "The theory of planned behaviour". *Organisational Behaviour and Human Decision Processes*. Vol 50(2), pp 179-211, 1991.

[25] R. Power. "CSI/FBI Computer Crime and Security," *Computer Security Journal*, Vol 17, pp 7-30, 2002.

[26] R.E. Ricer, A.T. Filak, and J Short. "Does a high tech (computerized, animated, PowerPoint) presentation increase retention of material compared to a low tech (black on clear overheads) presentation?" *Journal of Teaching and Learning in Medicine*. Vol 17(2), pp107−111, 2005.

[27] C.L. Anderson and R. Agarwal. "Practicing safe computing: a multimethod empirical examination of home computer user security behavioural intentions," *MIS Quarterly*. Vol 34(3), pp 613-43, 2010.

[28] R. Rogers. Cognitive and physiological processes in fear-based attitude change: a revised theory of protection motivation. In: J. Cacioppo, R. Petty, editors. *Social psychophysiology: a sourcebook*. New York: Guilford Press, pp 153-76, 1983.

[29] M.A. Hogg and D. Abrahams, Social identifications: A social psychology of intergroup relations and group processes. Routledge London and New York, 1988.

[30] S. Pahnila, M. Siponen and A. Mahomood. "Employees' behaviour towards IS security policy compliance," *Proceedings of the 40th Hawaii International Conference on System Sciences*, January, pp 3-6, Los Alamitos, CA; 2007.

[31] R. Richardson. CSI Computer Crime & Security Survey. CSI, 2008. Available from: http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf (Accessed 14 December 2009).

[32] C. Russell. "Security Awareness - Implementing an Effective Strategy," SANS Institute, *InfoSec Reading Room*, 2002.

[33] R.K. Sarkar. "Assessing insider threats to information security using technical, behavioural and organisational measures," *Information Security Technical Report.* Vol 15(15), pp 112-133, August 2010.

[34] B. Schneier. Schneier on Security. New Jersey: John Wiley & Sons, 2008.

[35] K.L. Smart and J.J Cappel. "Students' perceptions of online learning: A comparative study," *Journal of Information Technology Education*. Vol 5, pp 201−202, 2006.

[36] C. Pechmann, G. Zhao, M. Goldberg and E.T. Reibling E.T. "What to convey in antismoking advertisements of adolescents: the use of protection motivation theory to identify effective message themes," *Journal of Marketing*. Vol 6, pp 1-18, 2003.

Appendix B

This CD-ROM contains

1. A copy of an offline version of the information security awareness campaigns/training material and the assessment tests. Please note that the company logos and slogans have been removed in the interests of anonymity.
2. A copy of the research slide presentation sent to experts used in this study.

NB* The website on the CD-ROM is best viewed in Google Chrome. Please open the index page to view the site from the homepage.

Appendix C

This appendix contains copies of the questionnaires used in this research study.

1. Expert Review Questionnaire
2. Interview Questionnaire

Expert Review

Questionnaire

"An investigation of information security awareness"

Research at CEH

In

SOUTH AFRICA

2015

University of Fort Hare

Together in Excellence

Confidential

Thank you for your participation in this research study. Your responses will aid in the development of Information Security Policy Compliance Reinforcement and Assessment Framework. The following questionnaire is a medium that you can use to convey your professional opinions about the framework. Please be as detailed as possible with your responses. When you are finished, click on the "Submit Your Review" button at the bottom of this page or save and email.

Please enter the following information about yourself:

Your job title:

The name of the Company or Organization that you work for:

Today's Date: (example: 08 29 2015)

Please rank the following information security topics in regards to their relevance within your professional position:

	Very Important	Somewhat Important	Not Important	Not Applicable
1. Information security Policy.				
2. Information security awareness.				
3. Information security compliance assessment.				
4. Information security compliance reinforcement.				

5. Please explain the extent insider threat from naïve employees in your own opinion?

6. In your own opinion do you think awareness and training will change the employees behaviour towards security?

7. In your opinion what percentage of intent converts to behaviour and please elaborate why you feel that way.

8. In respect to the methodology used, do you think this was a good way of conducting this research?

9. To what degree, if any, do you agree or disagree with the proposed Information Security Compliance Reinforcement and Assessment Framework?

10. To what extent, if you do, do you agree with the findings of this study. Is it wat you expected?

11. Any suggestions of any improvements that could be made?

Please rate the following list of the frameworks attributes.

	Major Strength	Minor Strength	Major Weakness	Minor Weakness
12. Underlying Theories	☐	☑	☐	☐
13. Relevancy	☐	☐	☐	☐
14. Ease of understanding	☐	☐	☐	☐
15. Practicality	☐	☐	☐	☐
16. Critical thought applied?	☐	☐	☐	☐
17. Contribution to knowledge	☐	☐	☐	☐
18. Originality	☐	☐	☐	☐

19. presentation ☐ ☐ ☐ ☐

20. Overall Rating ☐ ☐ ☐ ☐

SUBMIT Your Review CLEAR All Answers

Last Updated: 15/12/2015

Interview

Questionnaire

"An investigation of information security awareness"

Research at CEH

In

SOUTH AFRICA

2015

University of Fort Hare
Together in Excellence

Confidential

Introduction

- *Interview questionnaire*
  - *This interview will take approximately 15 minutes;*
  - *All information collected will be presented in an analytical manner and, thus, no company specific information that may affect the organisation's goodwill goodwill will be disclosed and b] neither will any employee details be disclosed.*

Section A: Basic Personal Information

1. Gender group.

   Male [ ] Female [ ]

2. Age group

   Under 21 [ ] 21-30 [ ] 31-40 [ ]

   41-50 [ ] Above 50 [ ]

3. Which of the following reflects the respondent's job profile/role/title?

   Managing director [ ] IT technician [ ]

   Resources manager [ ] Administration [ ]

   Engineer [ ] Cad operator [ ]

   GIS operator [ ]

   Other (Please specify) _____

4. What is the respondent's employment status?

   Temporary [ ] Contract [ ]

   Permanent [ ] Service provider [ ]

   Other (Please specify) _____

5. How many years have they been with CEH?

   Under 1 year [ ] 1-3 years [ ]

   4-6 years [ ] Over 6 years [ ]

Section B: Company Background

1. How do they rate CEF's dependence on ICT?

   Very high [ ] High [ ]

   Low [ ] Not at all [ ]

2. How do their rate the level of ICT literacy at CEF?

   Very high [ ] High [ ]

   Low [ ] Poor [ ]

3. How do you rate the level of ITC security measures at CEF?

   Very high [ ] High [ ]

   Low [ ] Poor [ ]

Section C: Security Policy

**If answer to question 1(a) is not yes please don't ask them the remainder of the questions in this section*

1. (a) Does your organisation have a formal information security policy in place?

   Yes [ ] No [ ] Do not know [ ]

   (b) If yes, when was it first introduced to you?

   Recently [ ] On induction [ ] More than 3 years ago [ ]

   (c) When was it last communicated to you?

   Recently [ ] On induction [ ] More than 3 years ago [ ]
2. Has the security policy been formulated according to an established standard?

3. Has your security policy been modified/updated within the past 2 years?

   Yes [ ] No [ ] Do not know [ ]

   If yes, which one? _____

Section D: Organisational Security Practices

1. (a) Is there a formal structure in place to oversee and represent information security in your firm?

   Yes [ ] No [ ] Do not know [ ]

   (b) If yes what is the frequency of the meetings?

   Weekly [ ] Monthly [ ] Yearly [ ] Ad hoc [ ]

2. Are there comprehensive security awareness programmes in place?

   Yes [ ] No [ ] Do not know [ ]

3. Does the firm provide regular and structured training to its employees on information security and policy?

   Yes [ ] No [ ] Do not know [ ]

4. Is there any system in place to measure the success of and/or compliance with the security policy in this firm?

   Yes [ ] No [ ] Do not know [ ]

5. Is there an overall 'security officer' in charge of information security?

   Yes [ ] No [ ] Do not know [ ]

   If yes, who? _____

   Other matters arising:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

The End

Appendix D

This appendix contains copies of the ethical compliance documents for this research study.

1. Ethical clearance certificate
2. Employee informed consent form

University of Fort Hare
Together in Excellence

ETHICAL CLEARANCE CERTIFICATE
REC-270710-028-RA Level 01

Certificate Reference Number:	FLO051SGUN01
Project title:	**Employee Behavioural Model for Information Security Compliance: Closing the knowledge and behavior gap.**
Nature of Project:	PhD
Principal Researcher:	Tapiwa Gundu
Supervisor:	Prof S Flowerday

On behalf of the University of Fort Hare's Research Ethics Committee (UREC) I hereby give ethical approval in respect of the undertakings contained in the above-mentioned project and research instrument(s). Should any other instruments be used, these require separate authorization. The Researcher may therefore commence with the research as from the date of this certificate, using the reference number indicated above.

Please note that the UREC must be informed immediately of

- Any material change in the conditions or undertakings mentioned in the document
- Any material breaches of ethical undertakings or events that impact upon the ethical conduct of the research

The Principal Researcher must report to the UREC in the prescribed format, where applicable, annually, and at the end of the project, in respect of ethical compliance.

Special conditions: Research that includes children as per the official regulations of the act must take the following into account:

Note: The UREC is aware of the provisions of s71 of the National Health Act 61 of 2003 and that matters pertaining to obtaining the Minister's consent are under discussion and remain unresolved. Nonetheless, as was decided at a meeting between the National Health Research Ethics Committee and stakeholders on 6 June 2013, university ethics committees may continue to grant ethical clearance for research involving children without the Minister's consent, provided that the prescripts of the previous rules have been met. This certificate is granted in terms of this agreement.

The UREC retains the right to

- Withdraw or amend this Ethical Clearance Certificate if
  - Any unethical principal or practices are revealed or suspected
  - Relevant information has been withheld or misrepresented
  - Regulatory changes of whatsoever nature so require
  - The conditions contained in the Certificate have not been adhered to

- Request access to any information or data at any time during the course or after completion of the project.

- In addition to the need to comply with the highest level of ethical conduct principle investigators must report back annually as an evaluation and monitoring mechanism on the progress being made by the research. Such a report must be sent to the Dean of Research's office

The Ethics Committee wished you well in your research.

Yours sincerely

Professor Gideon de Wet
Dean of Research

25 February 2016

Invitation to participate in an information security research study

Dear CEF Employee:

I am inviting you to participate in a research study I am conducting towards the completion of a doctoral degree in Information Systems at the University of Fort, South Africa. The purpose of the study is to validate a framework called Information Security Policy Compliance Reinforcement and Assessment Framework.

How do I say yes?

If you would like to participate, email me [LINK] and I will put you on the list.

Why are you asking me, are others being asked too?

Everyone and CEB is being invited.

What's involved?

Within the period of 11months you will be asked to go through an information security awareness and training and complete a questionnaire afterwards (Maximum 3 sessions) this will be between 1 January and 30 November 2015, you will be sent a link to an information security online training site which has a lesson and an assessment questionnaire. The questionnaire will take about 30 minutes to complete. Responses will be pooled together, analysed, and then a group feedback session will follow up the next week. The number of sessions will depend on the results of the prior sessions.

You do not need to know anything about information security participate.

Will my responses be kept private?

Responses are anonymous – no one will know what you said. Findings will be shown at group level not individual level. However, all group responses will be posted so that participants can get ideas from one another. In addition, I will keep a list of all volunteer participants so that I can send study–related notices and reminders.

For research purposes, each survey will ask your technical skills and whether or not your job includes technical aspects. This is done to ensure that both technically inclined and non-technically inclined views are balanced.

Are there any benefits for taking part in this research study?

There are no direct benefits for participating. However, you may find it useful to learn how you can secure your information as well as your company's information asset. It will also be a refresher for the end user policy of you company which you signed on

induction and committed to adhere to. Once the research is completed, you may request a study summary.

What if I do not want to participate?

Participation is strictly voluntary.

Can I volunteer now and decide not to continue later?

Joining in not a compulsory commitment, you are free to withdraw anytime you feel.

If you want to volunteer please complete the attached form and return it to me, or if you have questions, please send me a note by Thursday of this week, close of business. I will aggregate all questions into an FAQ and send it out to all who contact me. I will need to know by Tuesday, January 11 th 2015 if you plan on participating

Regards

Tapiwa Gundu

Cell: +27726644507

Informed Consent Form

University of Fort Hare

I, the undersigned, confirm that (please tick box as appropriate):

1.	I have read and understood the information about the project, as provided in the Information Sheet dated _____.	☐
2.	I have been given the opportunity to ask questions about the project and my participation.	☐
3.	I voluntarily agree to participate in the project.	☐
4.	I understand I can withdraw at any time without giving reasons and that I will not be penalised for withdrawing nor will I be questioned on why I have withdrawn.	☐
5.	The procedures regarding confidentiality have been clearly explained (e.g. use of names, pseudonyms, anonymisation of data, etc.) to me.	☐
6.	If applicable, separate terms of consent for interviews, audio, video or other forms of data collection have been explained and provided to me.	☐
7.	The use of the data in research, publications, sharing and archiving has been explained to me.	☐
8.	I understand that other researchers will have access to this data only if they agree to preserve the confidentiality of the data and if they agree to the terms I have specified in this form.	☐
9.	Select only **one** of the following: • I would like my name used and understand what I have said or written as part of this study will be used in reports, publications and other research outputs so that anything I have contributed to this project can be recognised.	☐
	• I do not want my name used in this project.	☐
10.	I, along with the Researcher, agree to sign and date this informed consent form.	☐

Participant:

_____	_____	_____
Name of Participant	Signature	Date

Researcher:

_____	_____	_____
Name of Researcher	Signature	Date