TOWARDS AN INFORMATION SECURITY AWARENESS PROCESS FOR ENGINEERING SMEs IN EMERGING ECONOMIES

by

Tapiwa Gundu

TOWARDS AN INFORMATION SECURITY AWARENESS PROCESS FOR ENGINEERING SMEs IN EMERGING ECONOMIES

By

Tapiwa Gundu

Dissertation

submitted in fulfilment of the requirements for the degree

Master of Commerce

in

Information Systems

in the

Faculty of Management and Commerce

of the

University of Fort Hare

Supervisor: **Prof. S. Flowerday**

December 2012

ABSTRACT

With most employees in Engineering Small and Medium Enterprises (SME) 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 Engineering 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, technical preventative measures such as antivirus software and firewalls are proving to solve only part of the problem as the employees controlling them lack adequate information security knowledge. This tends to expose a firm to risk and costly mistakes made by naïve/uninformed employees. This dissertation 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, Protection Motivation Theory and the Behaviourism Theory. The process and model have been refined and verified using expert review and tested through action research at an Engineering SME in South Africa. The main finding was information security levels of employees within the firm were low, but the proposed information security awareness process increased their knowledge thereby positively altering their behaviour.

Keywords: Information Security Awareness; Information Security Behaviour; Information Security Training

DECLARATION

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

- The work of this dissertation 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 dissertation has not been previously submitted in full or partial requirements for an equivalent or higher qualification at any other recognised educational institution.
- 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.

_____ _____

Signature Date

ACKNOWLEDGEMENTS

I would like to express my gratitude to the following:

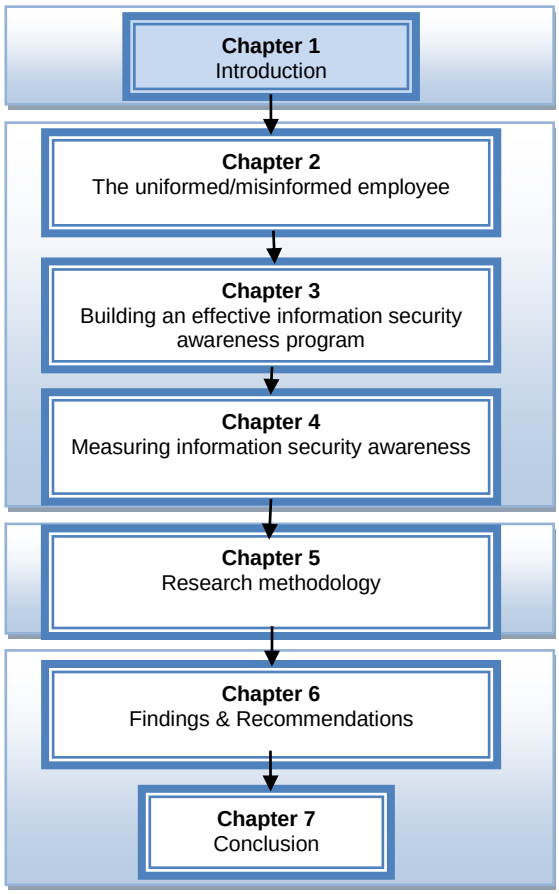
- To God Almighty for giving me the strength and protection. I could not have done this without your grace and mercy. '*Mwari makatendeka mazuva ose'*.
- To my supervisor, Prof. Stephen Flowerday. Thank you for being a mentor, teacher and friend. I learnt a lot through this experience. You are an excellent mentor who sees potential in people and help bring out the best of them.
- To the civil engineering firm where the empirical work was conducted.
- All the IS masters, doctoral students and staff for assisting whenever I needed help.
- To Sheila Hartwanger and Lauren Wainwright, thank you for assistance with language editing and proofreading.
- Finally, to my mum, brother and sister, thank you for all the love, support and prayers.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1 - INTRODUCTION



Chapter 1:

1.1. Background

Engineering Small and Medium Enterprises (SMEs) in emerging economies are investing significantly in their overall Information and Communication Technologies (ICTs). ICT is the technology used in the conveying, manipulation and storage of data by electronic means. ICT has become widely favourable by Engineering SMEs because of its fast processing and efficient data storage. This in the long run implies reduced costs due to increased efficiency. This ICT dependence has prompted major information security concerns for safeguarding of those information assets (Talaei-Khoei et al., 2012; ISACA, 2009).

Majority of these Engineering SMEs have information security policies providing a solid foundation for the development and implementation of secure practices (Talaei-Khoei et al., 2012). These policies present the rules that must be adhered to. Compliance with these rules, however, requires an understanding of not only the policies, but also how compliance helps the employee in his/her day-to-day activities.

When an information security policy is drawn up or revised and updated, implementation follows. However, for the information security policy implementation to be complete, it should be complemented with the implementation of an awareness program (Kabay, 2004). According to Peltier (2005), security awareness refers to sharing information with, educating, and training employees about risks to data, especially risks to the confidentiality, integrity, or availability of data, and about knowing what to do to protect it. In summary, security awareness means understanding that there is a potential for some people to deliberately or accidentally steal, damage, or misuse the data that is stored within a firm's computer system (Chipperfield & Furnell, 2010; Kabay, 2004).

Although information security awareness is only a single component of a larger information security program, its lack or weakness has implications on the realisation of overall information security goals (Eminagaoglu et al., 2010 Wilson & Hash, 2003, Pfleeger & Caputo 2011). Although this weakness that the employee presents can never be totally eliminated, a well-structured information security awareness campaign can help to reduce the risk to acceptable levels.

It is critical for employees to understand their role in reducing the risk and protecting information assets (Chipperfield & Furnell, 2010; Russell, 2002; Krutz & Russell, 2001). Such understanding can also be achieved by means of an information security awareness program.

Engineering SMEs rely heavily on digital information stored on computer servers. This information can include unpatented and patented private and confidential designs, client and employee personal information and in some cases trade secrets. This sensitive information is prone to both external and internal threats. Externally there are dangers

of data theft and commercial espionage from competitors or bad wishers. Internally, there is an even bigger threat of unsecure behaviours posed by ignorant insiders. The main hazard is that most employees, in particular those outside the technical fields, are not aware of the sensitivity of the information stored on their firms' ICT systems; yet they still have rights to read and write information stored on it. The debate around the origin of threats is supported by a global online E-Crime survey conducted by CERT in 2011. Respondents were asked who caused costly damages: insiders or outsiders. The results were close (insiders 33%, outsiders 38% and unknown 29%). The report also indicated that participants were not giving as much attention to insider threats as would seem justified. This is due to the assumption that information security is a technological problem to be solved by the latest technical innovations such as firewalls and antivirus software. This is, however, not completely true because innovative security programs tend to focus only on technical controls whilst human control is ignored (Russell, 2002). A firm can be bristling with firewalls and antivirus systems, but a naïve user can usher in an attacker in through the back door (Chipperfield & Furnell, 2010; Power, 2002).

Employees are often seen as the weakest link in the information security chain and hence this weak link needs to be strengthened. Educating and increasing employee awareness of expected security behaviours and how to respond to security incidents based on the firms' information security policy attempts to overcome this 'weakness' (Pleeger & Caputo, 2011; Van Niekerk & Von Solms, 2004; Schneier, 2000; Katsikas, 2000 in Stephanou & Dagada, 2006). The best Information Security policy and procedures are ineffective if there is no implementation of an Information Security awareness program or the awareness program implemented is not effective (Russell, 2002). If there is no awareness program the existence and contents of the firms' information security policy might not be known to its employees. 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. As such, Engineering SMEs should realise that employees, whether intentionally or unintentionally, are the greatest threat to information security, often due to lack of

knowledge (Brodie, 2008). Therefore the main reasons for implementing information security awareness programs are to ensure that:

- Employees (users) have knowledge of the existence and contents of the firm's information security policy and they adhere to it (Pflegger & Caputo, 2011; Peltier, ; Johnstone, 2001).
- Employees know their role in helping to protect the confidentiality, availability and integrity of the information assets (Talaei-Khoei et al., 2012; Stephanou & Dagada, 2006; Johnstone, 2001; Hunter, 2000).
- Employees understand why, how and from what/whom they are protecting the information assets (Eminagaoglu et al., 2010; Danchev, 2003; Van Niekerk & Von Solms, 2004).

In general, security awareness efforts are designed to change behaviour or to reinforce good security practices (Eminagaoglu et al., 2010; Wilson & Hash, 2003). Effective information security awareness programs may ultimately improve the firm's efficiency, as it will allow them to focus on techniques that improve their employees' intentions and ultimately encourage employees' security behaviour towards a more efficient enterprise (Stephanou & Dagada, 2006).

Following the implementation of information security procedures within the firm, there is a need to evaluate whether the information security awareness levels of the employees have changed (Kruger & Kearney, 2005). Most firms do not measure these levels because of problems associated with what should be measured and how it should be measured.

Although research has been done in the area of information security awareness, however, the literature lacks the study on the effectiveness of information security awareness methods on the basis of psychological/behavioural theories. Psychology is the science of mind and behaviour. Social psychology has been used for many years for research in the area of education, learning and human behaviour.

1.2. Problem Statement

Most Engineering SMEs do not have proper information security policies in place (Kabay, 2004). However, according to a survey by Richardson (2008), 68% of larger firms have security policies in place. According to Chipperfield and Furnell (2010), many of the firms that have these policies do not implement the information security awareness programs correctly in order to effectively secure their firm's information assets. This results in employees having limited information security knowledge. According to Schneier (2008), 62% of employees have limited information security knowledge and this helps exacerbate the information security awareness issues.

Therefore, employees need to understand how their actions can significantly impact the overall security position of the firm (Colwill, 2009; Krutz & Rusell, 2001). Insider threat accounted for approximately 44% of all occurring security incidents in 2008, this compared to 43% in 2007 and 42% in 2006" (Richardson, 2008). Therefore, the insider threat is undeniably on the rise and need immediate attention. However firms' mostly continue using technical controls like the antivirus and firewall technology to safeguard the information assets (Pfleeger & Caputo, 2011; Richardson, 2008). With such high figures Engineering SMEs should realise that there is a connection between what the employees know and how they conduct their behaviour towards security (Stephanou & Dagada, 2006). According to Colwill (2009), the 'people factor' and the technology together are the key to providing an adequate and appropriate level of security. Technology only safeguards the digital data and not the interaction between the data and the employee.

Having implemented an information security awareness program does not automatically guarantee that all employees understand their role in insuring the security and safeguarding of the information assets. It is necessary to develop a tool for measuring/evaluating the employee awareness levels (Kruger & Kearney, 2006). According to a survey by Richardson (2008), 32% of the respondents do not measure information awareness in their firms. This is usually because there is a challenge of what to measure and how to measure it (Kruger & Kearney, 2005).

1.3. Main Research Question

How can Engineering SMEs in emerging economies cultivate positive employee behaviour towards information security?

1.3.1 Sub-Questions:

i. What are the best ways to educate employees in order to raise their information security awareness levels?

ii. What are the attributes that affect employees' behaviour towards information security?

iii. How should information security levels be measured so as to assess the need for training, or assess the levels of awareness and effectiveness of a training session?

1.4. Objectives of Study

The objective of the study was to design, refine and validate an information awareness process that can be followed by Engineering SMEs when planning and implementing an information security awareness program.

This process will encompass a behavioural intention model that will assist in tempering with employee behaviour towards security and a measurement framework to assess the level of employee information security awareness. This measurement framework was based on Kruger and Kearney's (2005) information security measurement model.

This information security process could then be used as a benchmark guideline for Engineering SMEs with similar characteristics as the one it was tested on. The research has also added to the body of knowledge.

1.5. Significance of Study

One of the best ways to make sure that employees will not make costly unintentional errors in regard to information security would therefore be to institute a company-wide

information security-awareness program; this ensures that all employees have a solid understanding of firm's security policy, procedure and best practices (Brodie, 2008).

Security awareness training assists in tempering employees' attitude that security policies are restrictive and interfere with their ability to do their work. It also makes Engineering SMEs aware of potential internal and external security threats as there will be better reporting of incidences. The better the employees' understanding of security issues, the more they understand the importance of security and the ways in which security protects them and enables them to do their job in a more effective environment (Pfleeger & Caputo 2011; Johnston, 2001).

1.6. Initial Review of Related Literature

Hofstee (2006) notes that the purpose of reviewing literature is to give the researcher a better understanding of the research problem, theory base of work to be done and how the proposed research will fit into what has already been done. This study will review a variety of literature notably: books, journal papers, conference papers, white papers, dissertations, articles and the internet. In this review of literature, underpinning theories of the study will be discussed first and then all the other related research articles will also be briefly discussed.

This research bases its main argument on three theories, i.e. the Theory of Reasoned Action (TRA), the Protection Motivation Theory (PMT) and the Behaviourism Theory (BT). TRA suggests that a person's Behavioural Intention (BI) is depended on the employee'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 a behaviour. 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 favorable the attitude and the subjective norm, the greater the perceived control and therefore the stronger the person's intention to perform the behaviour in question (Fishbein & Ajzen, 1975; Hale et al., 2003; Miller, 2005). This research project seeks to influence the employees (attitude), as well as the management (subjective norm) towards better information security behaviour.

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 (Anderson & Agarwal, 2010). Information security awareness and training instill 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 (Rogers, 1983; Woon et al., 2005). It is composed of the following two items:

(i) Perceived vulnerability, i.e. an employee's assessment of the probability of threatening events. In this study, threats resulting from noncompliance with the firm's information security policy (ISP).

(ii) Perceived severity, i.e. the severity of the consequences of the event. In this instance, imminent threats to the firm's information security arising 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 (Woon et al., 2005). Coping appraisals are made up of three sub constituents:

(i) 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 study, it refers to the sorts of skills and measures needed to protect the firm's information asset (Bandura, 1991; Woon et al., 2005; Pahnila et al., 2007).

(ii) Response efficacy: this factor relates to the belief about the perceived benefits of the action taken by the individual (Rogers, 1983). Here it refers to the compliance with the information security policy as being an effective mechanism for detecting a threat to the firm's information assets.

(iii) 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 (Lee & Larsen, 2009; Anderson & Agarwal, 2010) as well as Information Security Policy (ISP) compliance (Herath & Rao, 2009; Pahnila et al., 2007).

The Behaviourism Theory (BT) was primarily developed by Skinner (1965), however, according to Skinner (1965); Watson coined the term "*behaviourism*." Critical of Wundt's emphasis on internal states, Watson urged psychology to focus on obvious measureable behaviours (Skinner, 1965). Watson believed that theorising thoughts, intentions or other subjective experiences was unscientific. It loosely encompasses the work of people like Thorndike, Tolman, Guthrie, and Hull. These investigators had similar underlying assumptions on the processes of learning. These basic assumptions are summarized 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.

Kruger and Kearney (2005) emanates that there is no simple answer to creating an effective and secure information environment, but Engineering SMEs should realise that one of the key aspects to better security is to raise the general level of information security awareness and to educate all employees on the basics of information security.

It is known that information security risk to a firm can never be totally eliminated (Flowerday & Von Solms, 2005). In fact, eliminating the risk would entail ceasing operations. However, although the risk employees expose the firm to can never be

totally eliminated, a well-planned security awareness program can help to reduce the risk to acceptable levels. Employees need to understand their role in protecting information and information assets in order to achieve a good information security culture (Chipperfield & Furnell, 2010; Russell, 2002; Krutz & Russell, 2001; Hunter, 2000).

Security awareness programs are typically divided into two different, yet related components: awareness and training. The goal of awareness is to raise the collective awareness of the importance of security and security controls. The goal of training is to facilitate a more in-depth level of user understanding (Krutz & Russell, 2001). An effective information security awareness and training program explains proper rules of behaviour for use of the firm's Information and Communication Technology (ICT) systems and the information assets. The program communicates ICT security policies and procedures that need to be followed. This must precede and impose sanctions imposed when noncompliance occurs. Users should be informed initially of expectations. Accountability must be derived from a fully informed, well trained and aware workforce (Wilson & Hash, 2003; Hunter, 2000).

Confidentiality, integrity and availability represent aspects of information assets being protected (ISO 27002, 2005). People, process and technology describe how this protection occurs. All three factors 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. Often it is just awareness that is the key to prevention and protection of valuable firm information assets, but most of the time these Engineering SMEs invest in the technological (physical) protection e. g. Antivirus and firewalls, but in reality employees control the technology; hence it is important to educate the employees in that respect (Pfledger & Caputo, 2011; Russell, 2002; Stephanou & Dagada, 2006).

Security awareness surveys are developed with the idea of measuring the current awareness level of employees. Such surveys will usually also point out common mistakes and misunderstandings among employees; this will immediately help improve

the quality of the program to be implemented (Danchev, 2003). Surveys are highly recommended periodically so as to monitor the information security awareness level trends.

Two distinctive challenges can be identified when developing a measuring tool and performing the actual measurements. These challenges are what to measure and how to measure it. Kruger and Kearney (2005) pointed out 3 attributes that can be measured and a model was developed on those dimensions, namely what the employees know (Knowledge), how they feel about the topic (Attitude) and what they do (Behaviour). The next sections give a brief outline of the research design and methodology followed for this study.

1.7. Research Design and Methodology

Research methodology is the process of systematically solving the research problem. It may be assumed as a science of learning how research is done scientifically. In it the various steps that are adopted by a researcher in studying the research problem along with the logic behind them are studied (Hofstee, 2006, Collis & Hussey, 2009).

1.7.1. Research Design

This study is phenomenologist/interpretivist inclined. According to Collis and Hussey (2009), positivistic and phenomenological paradigms are two extremes and only a few would operate in their pure forms. Figure 1.1 below shows the difference between the positivistic and the phenomenologist approach.

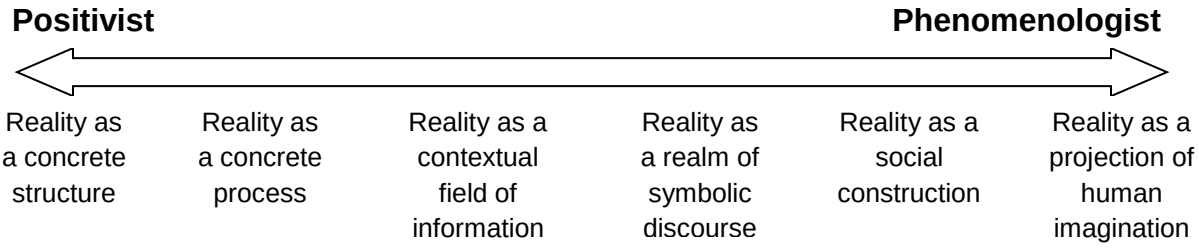


Figure 1.1: Continuum of Core Ontological Assumptions (Morgan & Smircich, 1980 in Collis & Hussey, 2009)

This research project falls in the Reality as a Realm of Symbolic Discourse when referring to the continuum of core ontological assumptions. In that stage, the social

world is viewed as a pattern of symbolic relationships sustained through a process of human action and interaction (Morgan & Smircich, 1980 in Collis & Hussey, 2009).

1.7.2. Research Methods

The methodology was based on the Action Research approach. This approach finds a situation of openness and cooperation, complex social processes, and the need to introduce changes into these processes and observe the effects during the process. Action Research innovation implies the creation of experimental situations which enables intervention during the process, observation of changes brought about, and creating learning situations (Schaffers et al., 2008).

"Action research allows researchers to address concerns that are closest to them, ones over which they can exhibit some influence and make change" (Schaffers et al., 2008). The Action Research was conducted at an Engineering SME specialising in civil engineering consultation based in East London (South Africa). The firm is heavily dependent on information systems and it has large amounts of information, which mostly consists of sensitive intellectual property (engineering designs, as-builts and GIS data) stored on its servers. This firm has all the typical characteristics of an Engineering SME in an emerging economy.

The researcher was actively involved with the employees at the engineering firm. The research was a cyclical process and it linked theory and practice. The action research was a form of field intervention that aimed at solving practical, real information security problems faced by Engineering SMEs. This supported Baskerville's (1999) view that action research is ideal for studying information system methods in a practical setting and empirically studying the applicability of the proposed new solution in practice and possibly its refinement.

1.7.2.1. The Information Security Awareness Process

Having discussed the theoretical background of the study, this section discusses the proposed information security awareness process in the form of a flowchart as shown in Figure 1.2.The process has four major processes listed below:

1. Drafting an information security policy.
2. Updating an existing information security policy.
3. Measure employee information security awareness levels and carry out a needs assessment.
4. Run information security awareness campaigns and training.

Process 1 and 2 are assumed they are already done, and this study focuses on process 3 and 4. Process 3 is based on a behavioural intentional model to be presented in this study, and process 4 is based on Kruger and Kearney's (2005) measuring model.

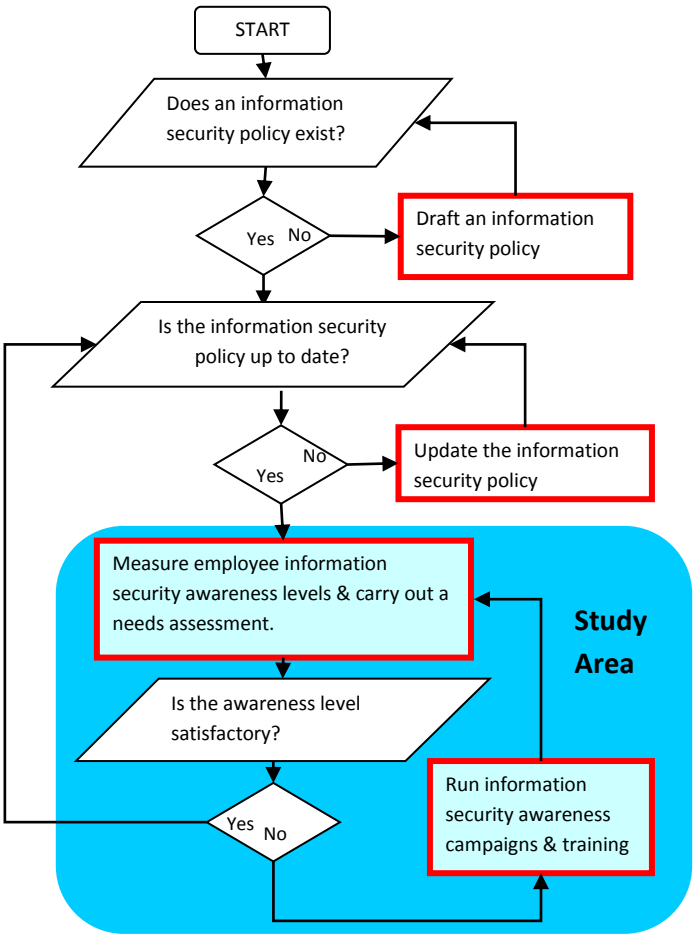


Figure 1.2: Information Security Awareness Process

1.7.2.2. The Behavioural Intention Model

The behavioural intention model that the campaigns and training in the proposed information security process are based on is presented Figure 1.3. Basing on the theoretical framework discussed in literature review section of this chapter, it can be agreed that the TRA, PMT and BT effect desirable behavioural intentions. The behavioural intention model presented Figure 1.3 fuses the theories together to come up with a model that enjoys the best of all theories.

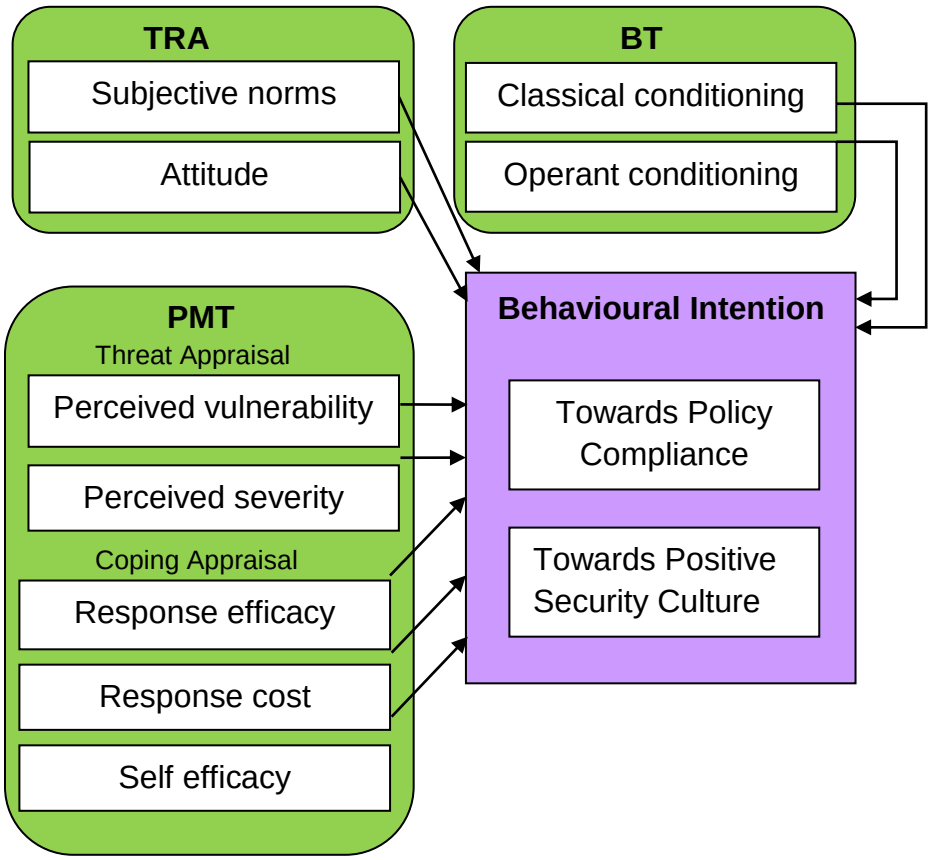


Figure 1.3: Behavioural Intention Model

This process was verified and refined through expert review and validated and further refined through action research.

1.7.2.2 Data Collection and Data Analysis

Data-collection techniques allow systematic collection of information about objects of study and about the settings in which they occur (Collis & Hussey, 2009). This research collected both primary and secondary data. Primary data was collected by the use of

web based surveys/tests, observations, and informal interviews. Secondary data was collected from published articles, books, internet and dissertations.

Data was collected by means of survey, observation and informal interviews. The data gathered from informal interviews and observations was not used for any calculations but was just used to assist in determining training topics for campaigns. The data from the online surveys was used for calculating information security awareness based on Kruger and Kearney's (2005) model. The model weighed knowledge, attitude and behaviour towards information security according to the importance scale agreed upon by the researcher and the firm's management. All the questions in the survey were based on Kruger and Kearney's three dimensions. The questions on the survey were structured in a way that extracted data reflecting on the employees' knowledge, attitude and behaviour towards information security within the firm.

Data analysis was also done based on Kruger and Kearney's (2005) model. The data for each cycle/iteration of the action research was analysed and then compared to results of the subsequent iteration in order to monitor changes in the employees' knowledge, attitude and behaviour of employees towards information security. According to the result, the process and model were able to alter employees' knowledge, behaviour and attitude.

1.8. Delimitation of the Study

Drafting an information security policy is the first sensible step that a firm can take if it wants to secure its information asset. However, for the purposes of this study it was assumed that the company already has a comprehensive information security policy in place and the firm where the action research was conducted already had an up to date information security policy, hence they was no need to draft or update one. Thus, this part of the proposed information security awareness process is not part of the study area.

They are two types of insider/employee threats; they are naïve mistakes and intentional insecurity from disgruntled employees seeking revenge. This study only focuses on the naïve mistakes made by the ignorant employee.

Lastly, information security awareness is just one of the important components to be considered when effectively implementing an information security program. For the purpose of this research the rest of the components will not be discussed.

1.9. Main Findings

Literature review revealed that insider insecurities are on the rise while outsider attacks are on the fall. However, most of the remaining outsider attacks are targeting the weaknesses of the ignorant employee. This is supported by Schneier's (2008) saying "Only amateurs attack machines; professionals target people."

Expert reviews concluded that, the proposed information security process was well-presented, could be easily followed, provided high technical quality, is unique, very comprehensive, has added new knowledge into the field of information security and has common originality.

The information security awareness process proposed in this research was tested in practice during the action research and proved to be able to increase employees' information security knowledge which in turn altered their attitude and which made them behave much more securely.

1.10. Structure of Dissertation

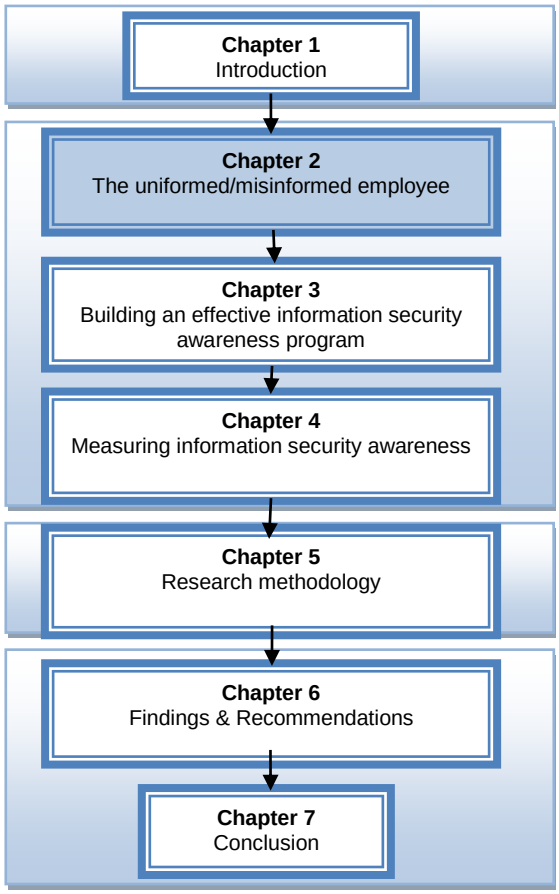
This dissertation is divided into seven chapters. Chapter 1 presents the introduction, problem statement, research objectives and a briefing of the methodology. Chapter 2, 3 and 4 consists of the literature study (secondary research). Chapter 5 presents the proposed information security process and the Behavioural Intention Model. It goes further to discuss the research methodology and the action research. Chapter 6 outlines the research findings and states recommendations that can be implemented by Engineering SMEs in emerging economies based on the findings of the action research. Chapter 7 is a summative conclusion that determines if the research has addressed the problems stated, and suggests any problems that may require further research.

1.11. Chapter Summary

This chapter highlights the risks an ignorant employee exposes the firm to and briefly explains the proposed information security process that may be followed to minimise these risks. This information security process is based on a behavioural intention model proposed in this research and an information security awareness measuring model adapted from Kruger and Kearney (2006). This chapter also summarises how the information security process was verified and refined.

This research study has been converted into a conference article (Please refer to Appendix A) and published in IEEExplore and has a journal paper under review. The research has been introduced in this chapter, the following chapter (Chapter 2) reviews literature on the ignorant insider and the risk they pose to the firm.

CHAPTER 2 - THE UNINFORMED/MISINFORMED EMPLOYEE (THE ENEMY WITHIN)



Chapter 2:

2.1. Introduction

This chapter seeks to identify types of employees and assess risks they expose their firms to. The multi-user era was brought on by the introduction of computers that can perform multi-processing and allow multiple users to log on at the same time. Most employees in Engineering SME's now have access to their own personal workstations which have become part of their daily functions. This has led to a high organisational dependency on Information and Communication Technology (ICT) for internal operations such as record-keeping, external transactions such as financial transfers, and communications of all types (e.g., email).

The increase in connectivity and resource sharing has led to the increase in the likelihood of intrusion, theft, defacement, and other forms of loss of the firm's important information (patented and unpatented private and confidential designs, databases, drawings, client/employee personal information and trade secrets). Engineering SMEs tend to be more concerned about vulnerability to external threats, although industry research suggests that a substantial proportion of security incidents originate from inside the firm (Sarkar, 2010; CSI survey, 2008; Etsebeth, 2006; Furnell, 2006; Stanton et al., 2004). The internal vulnerability is mostly from the uninformed/misinformed (ignorant) employee not behaving securely. The main hazard is that most employees, in particular those outside the technical departments, are not aware of the sensitivity of the information; yet in most instances they still have rights and access to the sensitive and highly confidential information stored on the firm's computer systems.

Engineering SMEs often assume that security is not an issue for them. In Engineering SMEs there is a significance influence of trust and ethics on workflow and thus security is not seen as a significant issue (Williams, 2009). Ironically, it is more important for Engineering SMEs compared to larger firms as employees often have multiple roles and thus have access to a variety of financial, organizational, customer and employee information as well access to multiple services such as the internet and email. Furthermore, in Engineering SME's there is less segregation of duties and thus less control over access to information (Williams, 2009). Whilst being exposed to the same threats and vulnerabilities as large firms, they do not have access to the same level of resources.

In today's highly networked systems environment, it is very difficult for firms to protect the integrity, confidentiality, and availability of information without ensuring that each employee involved shares the same security vision of the firm, understands their roles and responsibilities, and are adequately trained to perform them (ISO 27002, 2005). In order to assist in ensuring information security, individual users thus require knowledge regarding their specific role in the security process. This knowledge can be provided via education, training and awareness campaigns (Van Niekerk & Von Solms, 2010).

The challenge for firms is to ensure employees are aware of local security policies and procedures, as well as trained on how to implement these policies in a routine and consistent manner. Internal auditing and stringent security controls help reduce the threat of malicious employees acting out of spite or greed, but the defense against employees who simply lack the requisite experience or understanding necessary to safeguard information is only counterbalanced by an aggressive security awareness and training program. An hour it takes an employee to review an awareness presentation may be the difference between a secure organization and a multimillion Rand breach of security. This chapter will start by defining the insider, then the risk they expose the firm to, followed by a review of current insider risk statistics.

2.2. The Employee (Insider)

For many years Engineering SMEs have invested in preventive measures such as firewalls, antivirus software and antispyware in order to secure their information assets. However, these preventative measures are proving to only solve part of the problem and therefore, information security management is still an issue. Regardless of the technology deployed to protect information, employees still are the main problem as they control the technology.

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

- **Insider**: Current or former: employee, service provider or contractor.
- **Outsider**: Someone who has never had authorized access to an organization's systems or networks.

Figure 2.1 depicts the firewall barrier between the corporate network and the outside world.

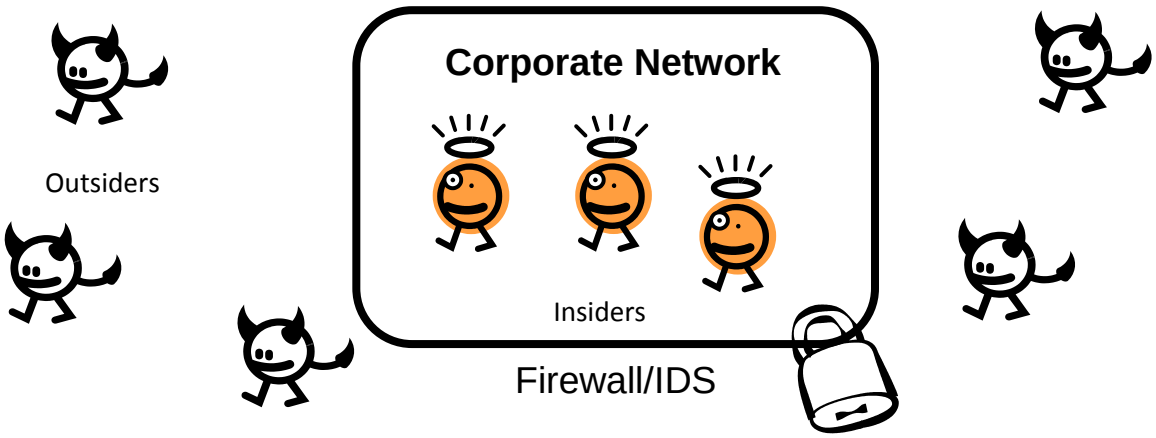


Figure 2.1: The Insider vs The Outsider

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 (Boeckeler, 2004). Traditionally firewalls were a hardware device, but today there are both hardware and software firewalls.

The Insider has unregulated access to some part or 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 attacks the target from behind or inside the system's perimeter defenses.

• The Insider can breach a system's perimeter defenses without arousing suspicion of network security personnel.

• The Insider has physical access to the system that compromises its perimeter network defenses.

One open issue is the case where an outside attacker gains access to the inside of a network by attacking or exploiting weaknesses in the network's perimeter defenses. For the purposes of this research, attention will only be given to insider although it is attributed that outsiders pose equally the same risk. The reason for this segregation is that the insider threat is usually taken for granted and firms usually do not have programs in place to minimise the risk they expose the firm to compared to outsiders where firewalls are being used to guard against intruders.

2.2.1 Corporate Citizenship of Insiders

According to Sarkar (2010), insiders can be divided into pure insiders, insider associates and inside affiliates. The pure and associated are discussed briefly below and the affiliates are self-explanatory.

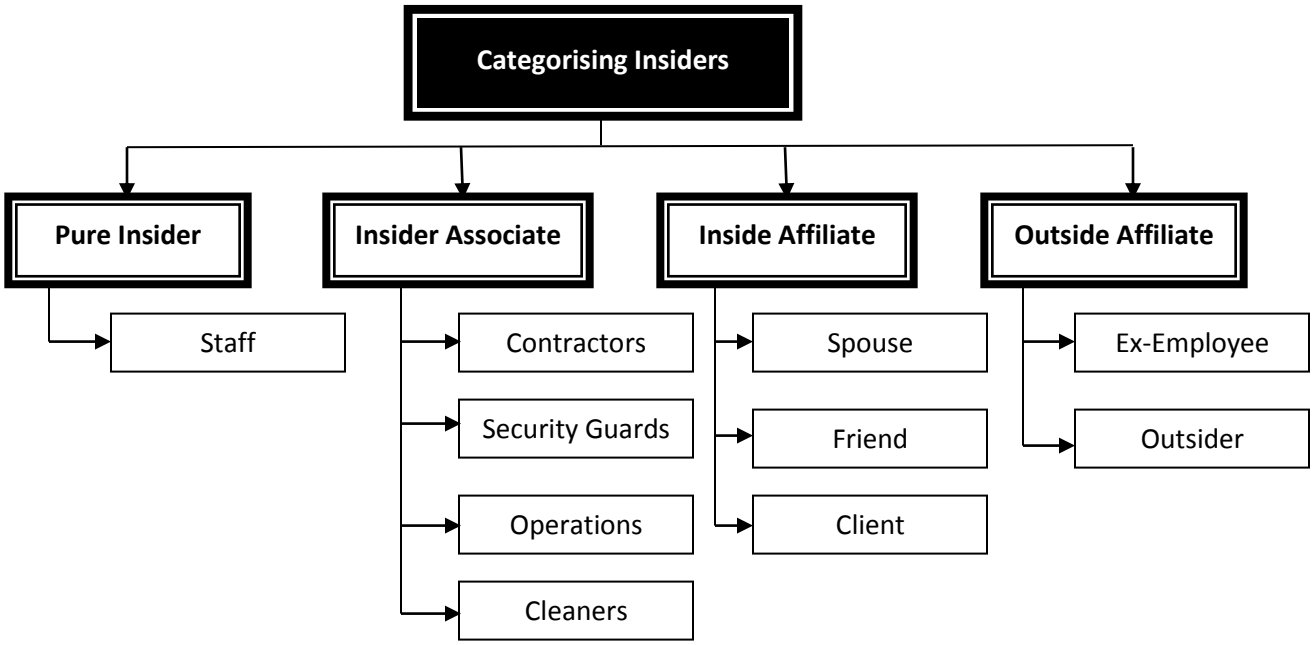


Figure 2.2: Categorising Insiders (Sarkar, 2010)

2.2.1.1. Pure Insider

Pure insiders are full-time & part-time employees with necessary privileges like, keys, access cards, and network logon made available to them in order to perform their job function (Sarkar, 2010). Employees pose the greatest risk to the firm in terms of access and potential damage to sensitive and private information systems. As vetted members of the firm, employees are entrusted and are expected to have interest in the productivity and success of the firm. After recruitment, employees are considered "members of the family" and are therefore often above suspicion. This makes them the last to be suspected when systems malfunction or fail (Shaaw et Al, 1998).

In addition, former employees often retain sufficient access to the firm to remain an "insider" threat. Former employees are individuals who no longer work at the firm but still have access to information resources directly through "backdoors" or indirectly through

former associates. When an employee is having conflicts with an employer, or anticipating termination of their contracts, they may prepare backdoor access to the computer system, alternative passwords, or simply hoard proprietary data for later use. The number of cases in which separated employees have returned to revenge on their former employers indicates a need for improved management of the employee termination process. This is particularly the case in episodes involving large numbers of layoffs. Such reductions can result in a pool of disgruntled employees and former employees with access and motivation for revenge (Shaaw et Al, 1998).

2.2.1.2. Insider Associate

Insider associate are often third party personnel, for example: Contractors, Partners, Consultants Cleaners, Security Guards and Temps, or Suppliers with limited authorised access like access to a facility or restricted access to networks. They might have access to employees' desks, bins etc. They may find sensitive information/documents on the desks like usernames and passwords left in bits of paper under keyboards, stuck on monitors, or may plant key logging devices to retrieve sensitive information.

Contractors, partners, consultants and temps are separated from employees because they are often not, in practice, subjected to the same screening and background checks. Most firms within have little control over the pre-employment procedures and hiring practices utilised by a contractor or consulting group. This is true even though contractors and consultants (and sometimes temps) often have highly privileged access to the firm's information assets due to the increase in outsourcing of expert personnel. While the contracting organization is well within its rights to require contractors to screen the employees that will be working within the organization or provide a separate screening process for contracted employees, such steps are rarely taken, putting the firm at risk. The hiring of former hackers by some computer security consulting firms further increases the risk of security compromises. Employers have also consistently underestimated the ability of contractors and consultants to take advantage of even limited access to important systems (Shaaw et Al, 1998).

2.2.2 Attributes of the Insider

The *Insider* can be described by a variety of attributes. These attributes include but not limited to: access, knowledge/skills, risk, and process.

2.2.2.1. Access

Resources, like storage and databases are now shared and could be accessed remotely in a distributed fashion. This has brought in the problem of ensuring that only authorised users gain access to these resources. In trying to ensure this, technical controls such as authentication and access controls are being implemented (Du Plesseis 2002).

2.2.2.2. Knowledge/Skill

Firms have different departments and in those departments employees have different rankings, depending on their levels on knowledge, experience and skill. It should therefore be taken into account that these employees will obviously have different backgrounds in terms of knowledge and skill with regard to information security, hence concluding that they will behave in the same manner so ensure the firm's assets are secure would not be accurate (Pfleeger & Caputo, 2011)

2.2.2.3. Risk

The *Insider* is very risk-averse. The risk the employees expose the firm to, are not the same, as they depend on the levels of information security awareness of the particular employees and the type of information they have access to (Colwill, 2009).

2.2.3. Motives Behind Attacks

The motives behind attacks to the firm's information assets include unintentional insecurity/naïve mistakes and intentional insecurity/dangerous tinkering. Figure 2.3 below summarises motives behind attacks.

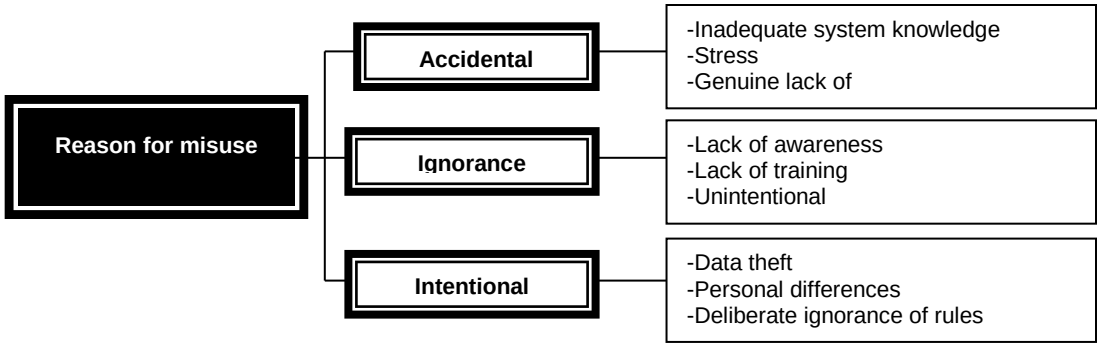


Figure 2.3: Reason for Misuse (Magklaras and Furnell, 2001)

2.2.3.1. Unintentional Insecurity/ Naïve Mistakes

These can either be accidental or out of ignorance. Below are a few examples of costly naïve mistakes that occurred between January 2008 and April 2010, and this list is just a small percentage of security breaches encouraged by a lack of an established security awareness program:

Example 1: An employee at Ohio State University's Agricultural Technical Institute accidentally emailed sensitive information on 192 faculty and staff members to almost 700 students. The email contained a spreadsheet containing among other things salaries and Social Security numbers (Insecure Magazine, 2008).

Example 2: The University of Texas Health Science Center at Tyler suffered a data breach when a contractor mailed 2000 envelopes containing the Social Security Number on the envelope (Insecure Magazine, 2008).

Example 3: Back here at home an East London Hospital Complex employee, made the patients details server accessible on the internet. This disclosed detailed information on patients who had been to Frere Hospital including their telephone numbers, home addresses, dates of birth, ID numbers, marital status and occupation. Next of kin names and contact details were also recorded. The accessibility of the records is in clear breach of the Patient Rights Charter to which all hospitals subscribe (Med-e-News, 2010).

These examples are **not** acts of an insider (employee) attempting to discredit the firm or make profit by selling confidential data. Each situation represents an employee that has either been improperly trained on security, or lacks the security awareness necessary to consider the consequences of their actions. These employees had nothing to gain by committing these breaches. Had these offending parties been trained on secure processes and aware of activities that could lead to a security breach, they could have prevented poor publicity and potential financial liability their firms incurred.

2.2.3.2. Intentional Insecurity/ Dangerous Tinkering

Employees who cause damage use their knowledge and access to information resources for a range of motives, including greed, political protest, terrorism, revenge for perceived grievances, ego gratification, resolution of personal or professional problems, to protect or advance their careers, to challenge their skill, express anger, impress others, or some combination of these concerns (Elliot, 2011; Sakar, 2010; Shaaw et Al, 1998). This can be illustrated by Figure 2.4 below:

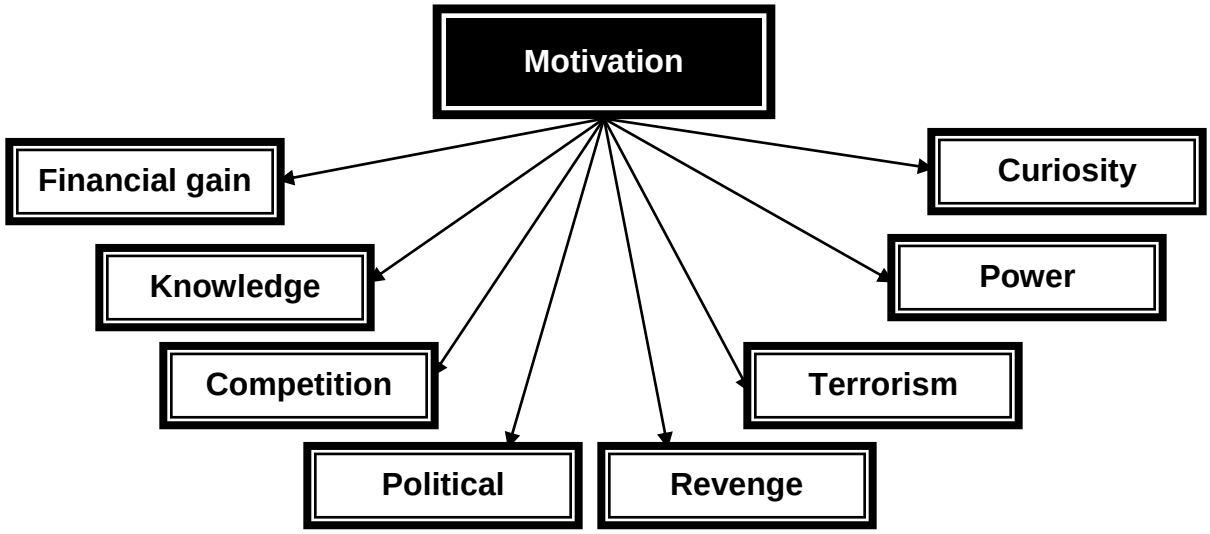


Figure 2.4: The components of motivation (Sakar, 2010)

The four case examples below serve to illustrate intentional insecurity:

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

Example 2: Two former Coca-Cola employees were sentenced to serve 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, got a five-year term, according to a news release from the U.S. attorney's office for the Northern District of Georgia. Both were ordered to pay $40,000 in restitution (CNN, 2007).

Example 3: New Jersey police arrested and charged nine people, including seven Bank of America employees and a man known as Lembo, who operated DRL Associates, the bogus collection agency. Customer account numbers and balances were allegedly sold to Lembo, who then sold the information to collection agencies. Lembo paid $10 per name, convincing the bank employees that they wouldn't get caught (CNN, 2005).

Example 4: Donald Burleson, a computer programmer for USPA & IRA Co., a Fort Worth securities trading firm, designed a virus after being reprimanded for storing personal letters on his company computer. The virus was designed to erase portions of the Company's mainframe and then repeat the process if a predetermined value was not reset in a specific location. After being fired, Burleson used a duplicate set of keys to return to the facility at 3 a.m. and employ an unauthorized backdoor password to reenter the system and execute the virus (Gann, 2006).

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

Risk is "the likelihood that a threat materializes" (Stoneburner at al, 2002). To some degree risk is unavoidable and firms must accept a degree of risk. Elky (2004) attributes that risk is not only caused by humans, and identifies the following as some 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, unauthorized access).
- **Environmental Threats** : power failure, pollution, chemicals, water damage

Risk is seen as the probability of loss or damage. Risk management is a function of three variables: criticality, vulnerability and threat. The first element is criticality; how important is this asset to the firm? The second element is vulnerability; in what ways can the asset be compromised, exploited, damaged or destroyed? The third element is threat; 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

(Leson, 2005, US DOD, 1999). Figure 2.5 below illustrates how vulnerability, threat and criticality tie up to form risk.

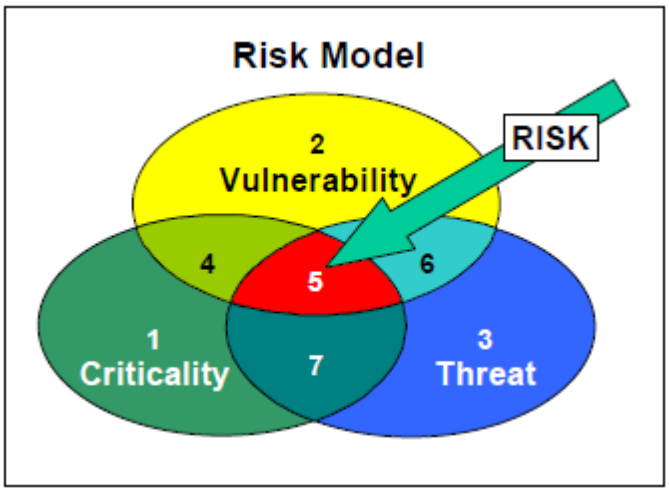


Figure 2.5: The Risk Model (US DOD, 1999)

Risk management involves understanding the value of the information to the firm and others putting in place protective measures corresponding to the value of the information (US DOD, 1999). Any response needs to be suitable to the threat posed. For instance, 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 what action is taken, for example shutting the window after the rain has stopped and has already come in, is too late. With the increasing interconnectedness of systems, it is important to respond rapidly to contain the threat and limit further damage.

2.3.1. Information Security Risk Analysis

Caelli, Longley and Shain (1989) define risk analysis as: “The minimising of risk by effectively applying security measures commensurate with relative threats, vulnerabilities and values of resources to be protected. The value of the resources includes the influence on the firm, the automated system supports, and the influence of the loss or unauthorized modification of data”. Acceptable information security risk levels can be thought of as a tradeoff with the corresponding costs of protection. It is important to have an economic evaluation of the security investment to avoid the costs and risks of a security breach (Tsiakis, & Stephanides, 2005).

Kwok (2009) reckons it's almost impossible to determine how much security a firm needs to keep its systems safe from intrusions and in some cases, information security risk analysis raises more questions than they answer. Nevertheless, the benefits of an information security risk method play a very important role in a firms success. Information security risk analysis can help firms to measure their economic loss due to problems occurring in their information security processes (Finne, 1998). Information security risk analysis provides firms with increased knowledge and more depth of understanding regarding their expected loss due to security failure (Gerber, von Solms, & Overbeek, 2001). Firms must ensure that the information security risk methods methodology employed corresponds with international best practice and is appropriately adapted to their particular environment (Albert & Dorofee, 2003; ISACA, 2009; Alnatheer, 2009).

2.3.2. Risk Assessment

Risk assessment is useful in determining the extent of the potential threat and risk the employee is exposing the firm to (Williams, 2008). The output of this process helps to identify appropriate controls for reducing or eliminating the risk. The insider threat need not be malicious; it may be uninformed, driven by culture, mistakes, errors, or be attributed to a lack of policy and procedures. Addressing these issues requires consideration of both technology and people; it requires an encompassing security governance approach. The governance approach is a method of pursuing strategic goals by balancing risk with return on investment. It includes accountability and allows for demonstration of appropriate practice and integrity and means that everyone in the firm is involved (Williams 2008).

Identification of what to protect and its value to the firm are important. ***Risk = Value x Threat x Vulnerability*** is an accepted risk assessment equation (Stoneburner, 2002). The greater the value of the information to the firm, the greater the risk of damage to the firm if any threat and vulnerability exist. However, often the perception of threat is over estimated in relation to the value of the information and therefore a perceived risk is given more credence and attention than is required to protect that information (Williams,

2008). What should also be considered is the impact of any effective threat particularly in terms of workflow and ability to continue with the organization's primary function. Therefore, a defined process for risk assessment and thus a balanced response to treats needs to be predefined.

2.3.3. Threats and Vulnerability Identification

With the increased capability and reliability of personal computers and the availability of end-user packages, the power and therefore responsibility has shifted to the end-user. The users that now have all these capabilities are generally not trained in the information technology field and therefore do not possess the skills to use them in a secure manner (Thomson, 1998). Using passwords to control access to data would be useless if the computer housing the data could be carried out the door because a user left the door unlocked, or if the user posted the password next to the screen. Operational controls are now needed to dictate and ensure that users operate in a manner that would not undermine these physical and technical controls in place (Du Plessis 2002).

Vulnerability is a measure of the exploitability of a weakness that encompasses the business processes, communication systems, and information technology supporting the mission of the firm. An Insider threat is the potential for a particular insider threat source with the Motivation, Capability, and Opportunity to successfully exploit a particular vulnerability or compromise a system (Sarkar, 2010).

The public may not be aware of the insider threats because almost three-quarters (72%), on average, of the insider incidents are handled internally without legal action or the involvement of law enforcement. However, cybercrimes committed by insiders are often more costly and damaging than attacks from outside (CSO Magazine, 2010).

William (2008) indentifies threat as human error, intellectual property compromises, unauthorised access, information extortion, sabotage, theft of information, disruption in availability and software attacks. However Sarkar (2010) identifies them slightly different as shown by figure 2.7 below.

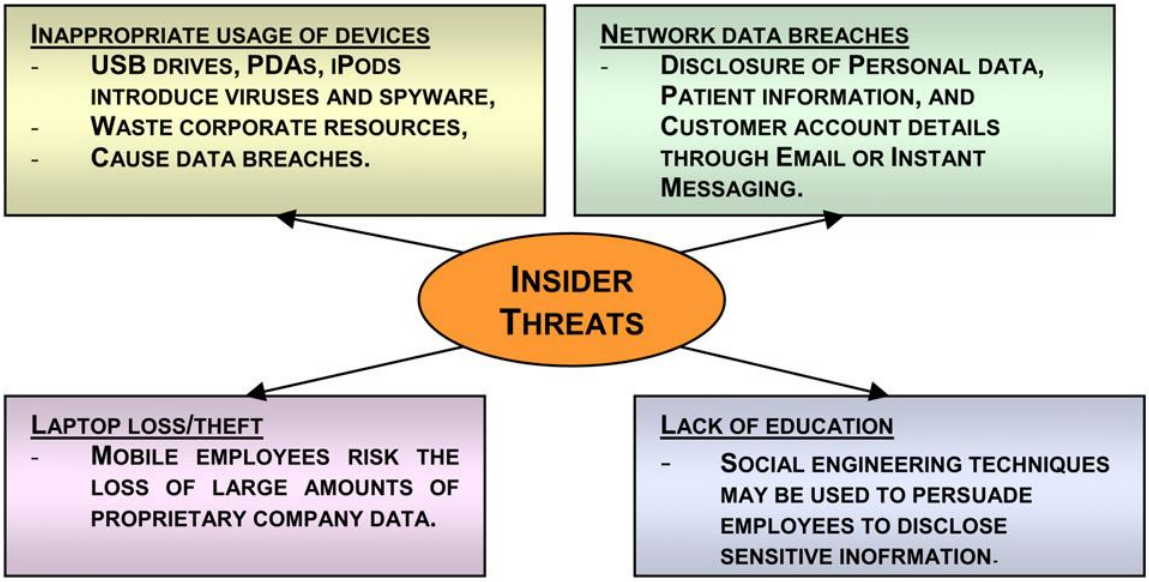


Figure 2.6: Possible Insider Threats (Sarkar, 2010)

The uninformed employee can cause risk to the firm's information asset by visiting malicious software (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.

- ***Malware***

Malware is contaminant software designed to secretly access a computer system without the owner's informed consent (www.antivirusworld.com, 2012). Software is considered to be malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, scareware, crimeware, most rootkits, and other malicious and unwanted software programs. Preliminary results from Symantec published in 2008 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 2007 alone exceeds the total 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.

- ***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 (US-CERT, 2011). Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to fool 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.

- ***Passwords***

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

1) Does not contain any words found in a dictionary
2) Does not contain any words that are of significance to the user
3) Does not contain any numbers that are of significance to the user e.g. birthday
4) Is not a variation of 1,2 or 3

For example “cowboy” is an example of a weak password, however changing it to “CowB45oy” does make it a much stronger password.

Lastly is never a good idea for employees to keep their passwords on a post-it note underneath their keyboard or screen. They should not bother having passwords in the first place if they are going to have them accessible anyone who wants them.

- ***Social Engineering***

Social engineering is the act of exploiting human weaknesses and manipulating people into performing actions or divulging confidential information, rather than by breaking in or

using technical cracking techniques (US-CERT, 2011). This could include calling the firms secretary and pretend to be the firms IT technician, make up a lie like there is regular maintenance scheduled on her computer after hours so she needs to give her password and she unsuspectingly divulges her password (Newbould & Furnell, 2009). Social engineering is a legitimate strategy for serious hackers, and some of the most infamous and successful hackers have been very skilled at it (Boeckeler, 2004).

When exploiting greed, the attacker suggests to the victim that they will get a large amount of money for sending a small amount of money first, usually explained as a release fee, bribe or legal fee. Other forms of this attack can consist of the attacker imitating a victim of a recent natural disaster – trying to exploit the reader's sympathy. Although most recipients of the emails do not respond there will always be a small but tangible proportion that does.

In Engineering SMEs there is often a high level of trust in the organizational culture and this trust in not conducive to effective security particularly when certain attack strategies like social engineering are reliant on such (Scott, 2009).

2.3.4. The Consequences of the Risk

Data loss, whether from internal or external sources, is still an overwhelming concern. The number of firms investing in data loss prevention (DLP) solutions leapt in 2009 to 44%, compared to 29% in 2008. Only six out of ten firms have an accurate inventory of the location of all their data and where and when it is collected and transmitted. Further commitment and investment in technology and education are required (SCMagazine UK, July 2010).

2.3.4.1. To the Employee

- **Dismissal from work**
- **Suspension from work**
- **Non/low bonuses**
- **Spam -** Spam 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**

2.3.4.2. To the Firm

Based on the findings of the survey by CERT - 2007 E-Crime Watch Survey (2007), it is noted that about 40% of the firms who were victims of e-crimes did not report for legal action, and according to the 2010 survey (CERT, 2010) the reasons for not reporting are: the damage level would not be significant enough to warrant prosecution; lack of evidence; the individuals cannot be identified and fear of negative publicity. The consequences the attacks have to the firm includes but are not limited to the following:

- **Data corruption** - An intentional modification, insertion, deletion of operating system or application system programs, whether by an authorized 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 intended purposes (Elky, 2004).
- **Denial of service -** Denial of Service (DoS) refers to intentional or unintentional assault on the availability of a system (Elliot, 2011).
- **Leaking/Theft of corporate data** - The unauthorized 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 the publications might have a negative effect on brand integrity or the reputation of the whole industry. Any insider attack when made public has a direct impact like resulting in loss of customer confidence, loss of customers to competitors, and huge financial loss of restoring normal service or cleaning up after the act (Sarkar, 2010).
- **Ransomware -** Criminals have the capability to encrypt a victim's hard drive leaving just a Readme.txt file telling the victim how to contact them to purchase the decryption key (Elliot, 2010).
- **Service disruptions**
- **Financial Losses**

- **Exposure**

2.3.5. Risk Mitigation

There are risk mitigation strategies that firms can use to minimise the risks from common security threats. Among the most effective of these are user awareness campaigns, implementing security controls, firewalls, intrusion detection systems and intrusion prevention systems, using anti-virus software, insurances and enforcing strong policies. The mentioned strategies fall in one of the following categories: transference, acceptance or avoidance. This research paper will have emphasis on avoidance although all of them are briefly explained below:

2.3.4.1. Transference/Sharing

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

2.3.4.2. Acceptance

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

so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured are 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 it would hinder the goals of the firm too much.

2.3.4.3. Avoidance

Risk Avoidance involves not performing an activity that could carry risk (Elky, 2004). An example would be not networking computers and not connecting them to the internet as it exposes the inside information to the outside world. Avoidance may seem like the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed, for example not entering a business deal to avoid the risk of loss also avoids the possibility of earning profits.

There are no 100% solutions for risk avoidance of information security risks and threats, but some of the following suggestions control these issues to some extent.

Antivirus Programs

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

Firewalls – hardware and software

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 it before it can enter your network. Most firewalls operate by a set of rules. These rules must be set up by the administrators of the network, and tell the firewall what to do under different conditions. There are different types of hardware firewalls, varying in sophistication. Organizations 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 is receiving everything that passes through the firewall. They are designed to spot suspicious activity, and alert the network administrators when necessary. In addition, they can help firms to learn from an incident and better prepare for the future (Boeckeler, 2004).

Software firewalls, like ZoneAlarm and BlackIce, run on Windows based personal computers. They actually include a lot of IDS functionality. Once installed, these programs monitor both what is coming into the computer, as well as what is leaving it. So they are able to detect all sorts of external activities directed towards your computer from port scans to a flood attack. Also, since they monitor traffic from a PC to the outside network, they can alert the employee to the presence of unknown malicious software, such as a virus or worm that is using your computer to conduct a DoS attack. These firewalls keep close track of which programs are allowed to access the Internet, and which aren't, but configuration is usually straightforward. Besides monitoring everything that goes in and out of a system, firewalls are also able to effectively hide computers on which they are installed from the outside Internet. A hacker can't break into a computer they don't know exists. As a result, when someone does try to conduct a port scan on a computer (really the IP address) running a firewall, they will learn nothing from it (Boeckeler, 2004).

2.4. Current Insider Statistics

Unfortunately no South African computer crime statistics exist at the moment. But generally speaking the computer systems are prone to the same threats so an

assumption will be made that the Australian, British and American statistics are similar to the South African.

According to CERT's 2007 E-Crime Watch Survey (2007), it indicates that insiders (34%) are fairly close to outsiders (37%) in causing most damage. Participants indicated that they were not giving much attention to the insider threats. According to this, there has been a drop in background checks (from 73% to 57%), account/password management policies (from 91% to 84%), employee monitoring (from 59% to 42%) and employee security awareness training (from 68% to 38%) as compared to the statistics for the year 2006. The CERT's 2010 E-crime Survey (2010) indicates while outsiders are the main culprits of cyber crime, insiders cause the most costly and damaging attacks.

2009 CSI computer crime and security survey (CSI, 2009). Key findings from the 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 2010 information security breaches survey shows a significant increase in the insider threat by 26% but investigators are still determined that 90% were a result of deliberate and malicious activity.

A 2005 survey commissioned by McAfee was revealing in terms of both employee behaviour and awareness. Amongst 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 PC.

Computer Economics, 2009 gives statistics about the types of insider misuse and how firms view the threats: Insider activities mostly revolve around stealing, destroying or modifying data. These activities can be classified as misuse under information systems, external websites and internal networks:

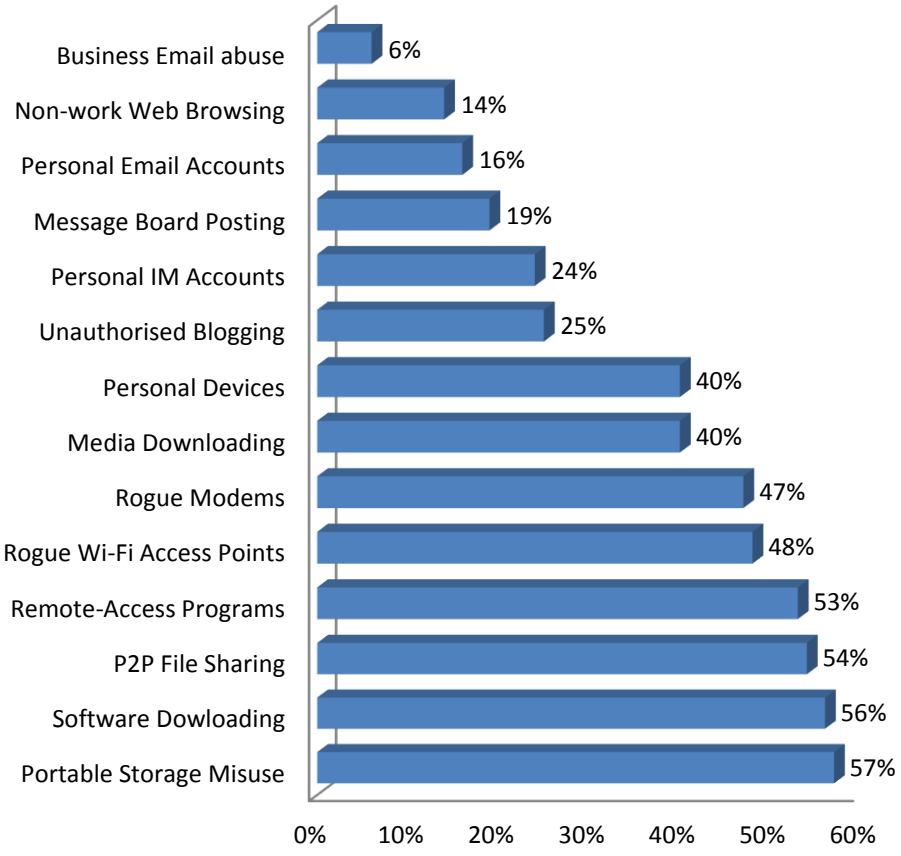


Figure 2.7: Percentage of Firms Viewing Type of Insider Misuse as Major Threat (Computer Economics, 2009)

The surveys clearly indicate that insider threats are becoming more of an issue and more wide spread than accounted for. One reason is the use of non-technical means like social engineering by insiders to gain unauthorised access and compromise firm's sensitive data. As firms are fortifying their perimeter, criminals are using more sinister means to gain access to the firm's proprietary information by 'planting' insider threats (Sarkar, 2010). The insider 'time bomb' is compounded by many factors like:

- Many firms do not report insider misuse, so the scale of the problem is hard to estimate.
- Employees are merging their working lives with their private lives.
- Firms are introducing a mobile work force, so the perimeter is becoming more porous, employees are carrying sensitive data on laptops, mobiles and USB's which when lost or stolen compromises the data (Sarkar, 2010).

2.5. Employee Information Security Awareness

The existence of a formal security policy does not necessarily mean that the employees will adhere (Herath & Rao, 2009). Subsequently they need to be 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 a firm's information security program; it is an initiative that aims at changing employee attitudes and behaviours by means of educating them about safe security practices (Veiga 2009). This ensures that employees realise the importance of security and 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 stored within a firm's computer systems and throughout the organisation (Kabay, 2005).

Awareness is the cornerstone of a security culture. Employees will make mistakes; forget to log off, passwords are not changed, and files are not updated. These are the realities of working in the computerised information society. The recognition of failures in security is vital in the protection of a system. This, together with consciousness of both internal and external risks, is important to drive behaviour and thus influence the security culture. Whilst awareness includes education and training, this is not the totality of it. It requires behavioural adaptation to create the appropriate response to the protection of information commensurate with its value to the organization (Williams, 2009).

Information security awareness can be compromised by risk perception. This is because decisions are based on knowledge and the perception of the risk (or lack of perception in most cases). The perception of lower risk means staff will ignore certain procedures and policies. This poor compliance may not be from malicious intent; it may merely be to work faster or more efficiently (Williams, 2009).

The use of standards to drive practice is accepted as good practice yet whilst there are standards for technical security (i.e. ISO 27002) there are no standards or guidelines for

driving awareness. It is however recognized as a significant factor in the development of a security culture (OECD, 2002).

2.6. Conclusion

Many in the information security profession agree that to achieve an improvement in information security the human factors issue must be addressed. This may be addressed by training, educating and increasing awareness but ultimately is only sustainable if a security culture can be promoted and adopted. The weakest link the security chain is still the human factor. What is required is not only to put good security procedures in place, but to create a community around practices that support sustainable change and adoption of best practice. In essence what is needed is the creation of an intuitive security culture. The information security profession is thus charged with facilitating this change. Arguably, this is a harder challenge than implementing sophisticated technical solutions.

Technical solutions can only protect information so far and thus the human aspect of security has become a major focus for discussion. Therefore, it is important for firms to create a security conscious culture. However, currently there is no or little established representation of security culture from which to assess how it can be maneuvered to improve the overall information security of a firm.

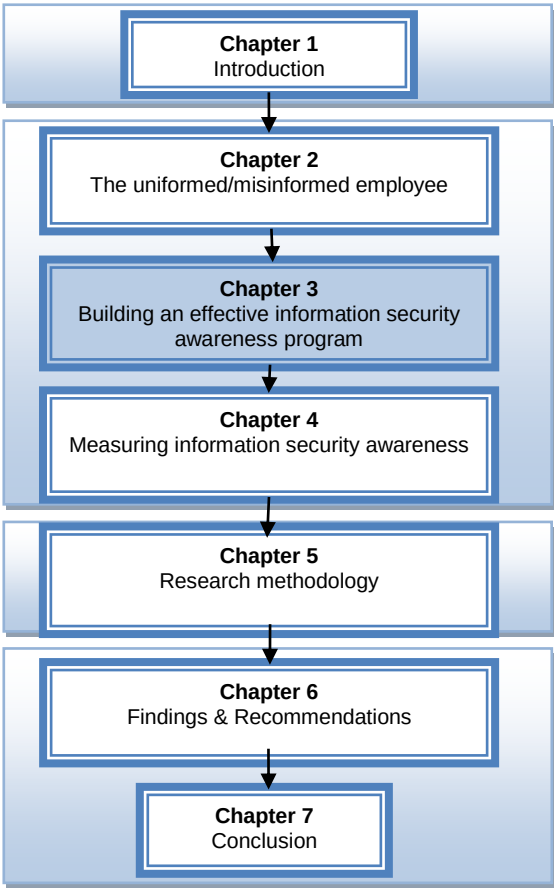
A firm's approach to information security should focus on employee behaviour, as the firm's success or failure effectively depends on the things that its employees do or fail to do. An information security-aware culture will minimise risks to information assets and specifically reduce the risk of employee misbehaviour and harmful interaction with information assets.

The majority of research on information security culture promotes the benefits of security culture without providing supportive evidence. As a result, there is little empirical work that investigates the relationship between information security culture and information security management factors in addition to cultural factors. This research attempts to reduce this gap and contribute to the behavioural information security literature by

exploring the influence information security awareness campaigns have towards the implementation and the adoption of information security culture.

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 its success. Creating an environment where every employee sees themself as a valuable part of the security culture will ensure its sustainability and increase the protection of important information. A balance between responsibility and monitoring needs to be attained. The objective of attempting to create or improve security culture in a firm is to ensure appropriate behaviour in regards to security is sustained long after information security training has ceased. The next chapter will discuss the methods of insuring a trusted information security aware environment.

CHAPTER 3 - ENSURING A TRUSTED INFORMATION SECURITY AWARE ENVIRONMENT



Chapter 3:

3.1. Introduction

This chapter illustrates how information security awareness programs are designed and how they assist in mitigating the risk exposed by the uninformed/ignorant employee. Information security awareness refers to a state where users in a firm are aware of, and ideally committed to, the firm's security mission (Pfleger & Caputo, 2011; Nosworthy, 2000; Schultz, 2004; Dlamini, 2009).

Increasing awareness of security issues is the most cost-effective control that a firm can implement (Drevin et al, 2007). Hinde (2002), suggests that the absence of awareness programs indicate a critical gap in effective security implementation. Security training and awareness programs are therefore a fundamental component of effective information security strategy. Security awareness and training can help firms to minimize

some of the damage caused by uninformed or misinformed employees (Eminagaoglu et al., 2010; Drevin et al, 2007).

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

A firm's management usually communicates formal company direction, rules and regulations using policies. These policies are usually either written (hard copies) or communicated verbally during employee induction. A copy might also be available on the firm's Intranet/SharePoint site. Information security policies provide a solid foundation for the development and implementation of secure practices within a firm. 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 in the employees' day-to-day activities (Johnson, 2006; Talbot & Woodward, 2009; Bacik, 2008; Dancho, 2003; Hone & Eloff, 2002; Von Solms, 2001).

When the information security team is ready to implement and train employees on the information security policy and safe information security practices, a mental image of the objectives to be accomplished should be created. The mental image should then be transformed into words and actions for presentation to the firm's employees. Effective communication should be a two-way process between the sender of information and a receiver of information (Bacik, 2008). Communication with the employee is usually by talking, watching, listening and observing activity. According to Wood (1994), information security awareness campaigns are the specific operational steps that employees must take to achieve the goals of the firm's policy. 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 (Johnson, 2006).

This chapter covers the roles and responsibilities of the employees, then discuses procedures of developing awareness of training material, followed by a discussion on the communicating techniques of the awareness material and finally the transition from information security awareness to culture is discussed.

3.2. Needs Evaluation

According to a survey carried out by multinational advisor group KPMG (1998), in conjunction with research group BMI-TechKnowledge, results showed that 66% of all respondents had limited information security knowledge and viewed information security as not important to the firm (Khan, 1999). Ten years later, according to Schneier (2008), 62% of employees still have limited information security knowledge. This helps exacerbate the information security awareness issues. CSI survey (2008) also revealed that 18% of respondents did not use awareness training at all, and a further 32% did nothing to measure the effectiveness of the approaches they used although the concept of Information Warfare, security awareness should be part of a firm's first line of defense.

Employees with 'little-to-no' prior security training or experience may suddenly be responsible for thousands of records with sensitive data as part of their job. Such understanding by way of a well-structured information security awareness program is therefore crucial in significantly minimizing the risk. Often the weakest link in information security is not the technology, but employees who control it. The weakness they present can never be totally eliminated, but a well-structured security awareness campaign helps to reduce the risk to acceptable levels (Krutz & Rusell, 2001; Johnson, 2006). However Wright et al., (2009) suggests that, an individual's ideas on security may vary over time and with different situations, which further complicates threat and vulnerability assessment initiatives. As a result, any awareness program needs to be continually measured and managed to keep abreast of changes in risk profiles (Kruger & Kearney, 2006). To keep the users current and their memories refreshed, an awareness program must be ongoing and be an integral part of firm's information security culture.

The development of information security policies and campaigns is a lengthy process that requires time, money and specialized knowledge. These constraints could prove prohibitive for small to medium sized companies and is a possible cause for low level awareness in such firms (Du Plessis, 2002). However, the small number of firms' implementing awareness programs and the low level of awareness within firms' suggests that these approaches are also ineffective (Du Plessis 2002).

3.3. Establishing Priorities

Alnatheer (2009) found that information security awareness was concentrated around the IT/IS departments and did not extend to all employees who have access to the firm's Information and Communication Technology (ICT) systems. It is important to understand that all employees, to a greater or lesser extent, need security awareness training. In the Armed Forces every soldier, no matter what they eventually do, goes through basic training. Similarly, every employee should have security awareness training, because every employee must act in a secure manner for the entire firm to be reasonably safe from 'employee-oriented' vulnerabilities. Firms seem not to realise the importance of information security awareness amongst all users (Von Solms & Von Solms, 2004). Eminagaoglu et al. (2010) and Alnatheer (2009) found that employee awareness is one of the greatest challenges that firms must face in order to achieve their required level of security.

3.4. Developing an Awareness and Training Strategy Plan

The first step in building an effective information security awareness program is to establish the existence of a security policy. The policy should comply with the ISO 27001:2005, ISO 9001:2000 or the COBIT. The policy should be written in a clear and concise manner, and accurately reflect the firm's overall posture towards security

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 (Habbard, 2002). Even though people know these things today, do they always wash their hands before eating, or even after doing something icky?" Unfortunately, not everyone does,

even when they know better. This highlights that the real challenge is not just to make employees aware, but also to help them change their behaviour. There is great need for firms to realise the connection between what their employees know and how they conduct their behaviour towards security (Stephanou & Dagada, 2008). They often overlook the reality that the firm is a custodian and therefore legally liable for the information which it collects, uses and maintains. Such responsibility requires excellent employee information security behaviour resulting from good information security culture (William, 2008). Security knowledge cannot help much if employees do not act on it.

An effective information security awareness and training program seeks to explain proper rules of behaviour when using the firm's computer systems and information. The program communicates information security policies and procedures that need to be followed. This must precede and impose sanctions imposed when noncompliance occurs. Employees must be initially informed of expectations such that accountability is derived from a fully informed, well trained, and aware employee (Herath & Rao, 2009).

3.5. Roles and Responsibilities

Experienced security personnel or willing non-security personnel within the firm can be made of great use by tapping them for articles, topical meetings, and presentations (Habbard, 2002). Their association can also be beneficial as respected organisational employees may add weight to the security awareness program. Another bonus of using in-house personnel for awareness training is that over time trusting relationships can be built around the experienced personnel.

There are many reasons to outsource security awareness training, as well. It is far easier and quicker to utilise the skills of a professional security awareness training company, if speed is of the essence (Habbard, 2002). Some companies specialise in particular aspects, such as awareness videos, newsletter creation, posters, or item customization (mouse pads, pens, *et al*). There are also some free sources for security awareness materials, which offer things such as screen savers, security best practices, or other educational materials. The firm can outsource almost any security awareness material it cannot or does not wish to provide online free sources or security awareness

vendors. Each program director must of course decide what is best for the firm's information security program.

3.6. Awareness, Training and Education

Information security awareness campaigns are divided into two different components, awareness and training. Awareness aims to raise the collective awareness 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 program seeks to explain proper rules of behaviour when using the firm's ICT systems (Herath and Rao, 2009).

However, awareness programs alone are not enough. While they may serve to get security issues onto the radar, they still do not ensure that staff is personally equipped to handle them. This is where information security training comes in, fostering the necessary knowledge and skills for employees to successfully protect information assets (Colwill, 2009; Furnell, 2009).

Training should not be a 'do not do this' program. The learning objectives of the program should be skills to support the corporate information security policy. Training should certainly promote the policy and procedures, but it should also be designed to instill a concept of best practice and understanding amongst the employees (Furnell, 2009). The firm can consider the program successful if all employees completing the training are entirely convinced and motivated by one fundamental belief: that information security is part of their responsibilities and that they have the skills to fulfill these responsibilities.

3.7. Developing Awareness and Training Material

3.7.1. Selecting Topics for Training

The main discussion of the awareness campaigns should be centered on the firm's security policy, it sets the security direction for the firm, and knowledge of this policy will help the employee understand what the firm is striving for in information security (Fowler, 2007). Such firm specific information would be impossible to cater for in a generic program. 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). Material would include security hot topics such as viruses, password construction, password management, laptop security while on travel, physical security, hacking, denial of service (DOS), Spoofing/sniffing data confidentiality, wireless security, home office, privacy, identity theft, internet usage, email usage, data backups, Intellectual Property Rights and encryption and the concept of social engineering.

3.7.2. Finding Sources of Awareness and Training Material

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

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

3.8. Techniques for Communicating Awareness Material

This section discusses techniques for communicating information security. Communication within a firm occurs in many different ways, but is usually described in terms of horizontal or vertical mechanisms. Horizontal (or sideways) communication is more informal and is between colleagues working at the same level (Chipperfield & Furnell, 2010). Many firms rely heavily upon vertical (downwards) communication, information passed from the top, passed down through line managers and in official communications.

Awareness material can 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 can contain numerous themes (Wilson & Hash, 2003). Regardless of the approach taken, the amount of information should not overwhelm the audience. Brief mention of requirements (policies), the problems that the requirements were designed to remedy, and actions to take are the major topics to be covered in a typical awareness presentation.

3.8.1 Persuasion Techniques

It is appropriate to consider different ways of shaping employee behaviour drawing upon knowledge from the management domain. The widely cited work in this context comes from Berlew and Harrison's categorisation of 'push' and 'pull' styles of influencing behaviour. Table3.1 shows a summary of the push and pull styles.

Push	***Reward and punishment***	A top-down approach based upon 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.
Pull	***Participation and trust***	Focuses upon 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, alongside the need for an associated group effort and commitment to achieve it.

Table 3.1: Push and Pull Styles (Chipperfield & Furnell, 2010)

Push approaches are by far the most common styles in the traditional promotion of security (Chipperfield & Furnell, 2010). For example, techniques around assertive persuasion can provide useful bedrock for understanding why security is needed, and many will at least recognise the issue from this basis. However, other styles may still be required to take them through to the stage of actually complying with the requirements, and it is here that the use of reward and punishment can create the framework within which the firm is able to formally lay out its expectations to staff. Chipperfield and Furnell (2010) recon that while the 'push' styles might succeed in getting employees as far as

the ‘obedience’ level, it is likely that alternative approaches would be needed to get them any higher.

Looking at the ‘pull’ styles, approaches hinged around participation and trust are unlikely to be that relevant in the context of promoting the broad security message, but could offer considerable value at the level of engaging individual stakeholders or small groups (Chipperfield & Furnell, 2010). Finally, the common vision would represent an aspect of achieving an overall security culture within the firm, and in that sense is necessary as part of setting the scene for this to occur.

3.8.2. Channels of communication

The BERR (2008) survey provides some relevant findings suggesting that majority of firms’ rely upon written materials of some form. However, simply developing and circulating a policy, or directing employees to an intranet page that details security procedures will not be sufficient to foster appropriate understanding and behaviour. An information security awareness program is necessary, the aim of which should be to focus employees’ attention on information security and move them from the ‘ignorance’ level to the ‘awareness’ level.

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 (Habbard, 2002). Before any communication is disseminated, the presenter needs to understand who the audience will be and why they are receiving the communication. Although the topic may not change, the way it is communicated may change depending on the audience (Bacik, 2008). The communication can utilise both formal and informal methods of instruction. Formal instruction methods include: security awareness tutorials, training courses, testing, formal presentations of security policies, or professional articles in newsletters. Informal methods might include brief newsletter articles, quick notes, lunch meetings, discussion groups, screen savers, posters, and physical reminders like mouse pads, pens, or tension squeeze balls. Figure 3.1 shows some of the ways the firm’s information security policy is communicated.

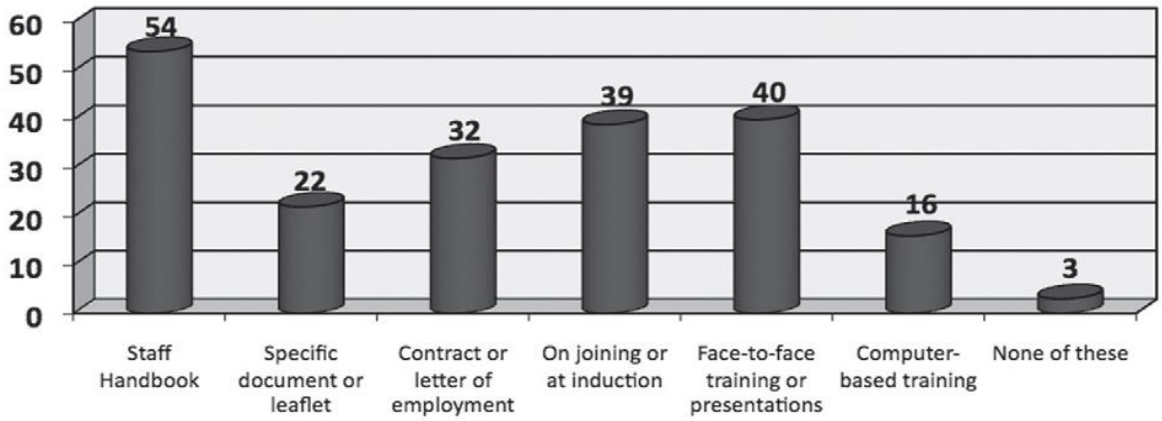


Figure 3.1: Information Security Policy Communication Methods (Berr, 2008)

The presenter/author knows the audience from working with them on a regular basis or knowing who they work for and the function of the business unit. The key to success in awareness/training is keeping the messages relevant and consistent, while varying the delivery mechanisms, to keep everyone interested. Both the delivery mechanism and the risk areas could change as the information risk profile changes. Channels of communication as seen in figure 3.2 are either written or verbal methods. Verbal and written communication methods will be briefly discussed in the following sub-sections.

3.8.2.1 Verbal

Face to face training/presentations

A common form of presentation is a lunch and learn. When a lunch and learn is held, the presenter normally prepares a logical method to communicate to the group. According to Bacik (2008), the audience knowledge and structure of a lunch and learn session enables the information security team to be able to present the session in three ways:

- **Tell and sell** - This is most effective for new employees. This involves the presenter lecturing the audience on what is being implemented and trying to sell the concept to the audience. This is where the presenter may be expecting defensive reactions or requires acceptance from the audience for the concept.
- **Tell and listen** - This is more effective when presenting a new topic or implementation. The presenter introduces new concepts and wants feedback from the audience as to how to improve or make the implementation easier, such as solving a joint business requirement.

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

3.8.2.2. Written

1. **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 tone is going to 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 we missing with this memo?
- Is the English used simple and straight forward?
- Has it been proofread before dissemination?

2. **Employee Handbook**

The employee handbook is normally one of the items that a new staff member receives on his or her first day and it usually gets placed on a book shelf and forgotten of. This is a static document until there is a major change within the firm, such as an enterprise acquisition or divestiture (Bacik, 2008). Information security policy architecture cannot reside within an employee handbook because it is a living architecture document and it changes depending upon the enterprise growth.

3. **Intranet**

The information security Web site, like the employee handbook, can become static if not maintained properly; it needs to be kept dynamic by updating it regularly (Bacik, 2008). The information security Intranet site should be a place to keep all staff up to date with

information on protecting the assets of the firm, with announcements of information security projects, tips, and tricks for the home networking environment, and for getting to know the information security team.

4. Computer based training (e-training/ e-learning)

Traditional classroom training is declining as a result of increased costs and e-learning's increasing popularity (Abdelariz et al, 2011). The information security team needs to assess the employees being targeted for awareness training and design the best method for access. The information security team needs to develop flexible and responsive sessions for the enterprise environment. Informal training needs to be relevant and immediate, possibly using the current work environment. The e-training sessions need to be short and valuable, so employees can be involved without taking time away from enterprise projects.

The most common training methods is e-communities comprise frequently asked questions, message boards with moderators, Web sites, and chat rooms (Abdelariz et al, 2011). Many firms know about these options for projects but have not extended them to the information security awareness environment. Super users and subject matter experts assist in keeping the material responsive, relevant, and current.

Another method of promotion of the e-learning is "brown bag" lunches or "meet the experts." These sessions are information sharing and displaying of critical awareness that employees need to protect the enterprise assets (Bacik, 2008). "Meet the experts" will permit staff to ask questions on how information security pertains to their work environment or to ask for better explanation on the existing information security policy architecture. The "brown bag" lunches and "meet the expert" sessions will also allow the information security team to mentor employees in becoming more familiar with the information security team and becoming more comfortable with the information security policy architecture.

5. Informal Methods

Johnson (2006) identified useful and effective methods communicating information security awareness as promotional and informational methods; these are listed in figure 3.2:

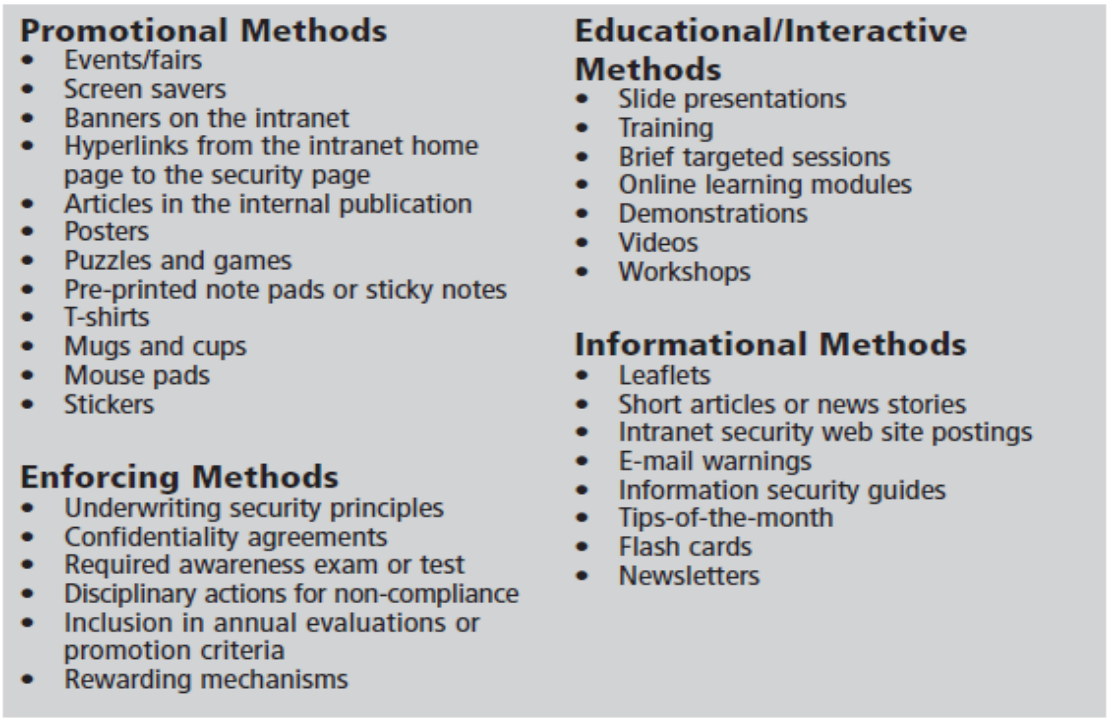


Figure 3.2: Information Security Communication Methods (Johnson, 2006)

Habbard (2002) and Albrechtsen have similar informal methods lists, they include brief newsletter articles, quick notes, lunch meetings, discussion groups, screen savers, posters, and physical reminders like mouse pads, pens, tension squeeze balls and games.

3.8.3. Barriers to Effective Communication

The main aim of an employee information security awareness campaign is to make sure that the firm's information security policy is well understood and followed by all employees in the firm. The audience (employees) tends to check the credentials of the information security personnel for them to accept the information communicated (Bacik, 2008; Chipperfield & Furnell, 2010). The personnel therefore need to have decent

credentials. Credentials do not necessarily mean a bunch of certifications after their name. Credentials can be “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 cause different meanings to different people
- Emphasis or specifying certain words
- Incorrect or inappropriate usage of words and phrases
- Skipping vital background information assuming the audience has the knowledge
- Homonyms or words with the same spelling and sounds, which have different meanings, for example, *their* or *there*

Before the message is given 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 means because the information security team relies on the employee’s perception or interpretation of the message communicated.

3.8.3.1. Identified Employee Issues With Respect to Information Security Policies

Literature investigation into the existing information security policy implementation identified a number of issues. The issues presented are not limited to the policy documents themselves, but include issues which impact policy effectiveness and the information security awareness of the employees in the firm. Talbot & Woodward (2009) summarised them with the following list, with further information relating to each finding presented below:

- A culture of ignoring policies
- Minimal awareness of policies
- Minimal policy enforcement
- No compliance program
- No formal non-compliance reporting

- Apparent inconsistent enforcement across the whole firm

The issues above reveal how 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

A culture of ignoring policies

The history and how the firms have dealt with policies have resulted in a culture within the firm in which employees ignore policies which they do not wish to comply with. This is a major hurdle which needs to be addressed before any policy implementation can be effective (Talbot &Woodward, 2009). Currently a number of information security policies are scoffed at when they are ready for implementation. Comments such as “who cares about the policy, you can’t enforce it” are common place within firms. Most employees view policies as a means of disciplining them or hindering their development and operational advancement.

Minimal awareness of policies

Most firms have their corporate polices on the intranet and in their contracts of employment. These policies include the information security policy but employees seem to be unaware of their presence. Awareness of relevant policies is next to non-existent. Making the signing of policies mandatory for employees on induction does not ensure the employees have read/understood the contents of the document (Johnson, 2006). For those that have read it, refreshers on this policy contents are still of great importance.

Minimal policy enforcement

Policies, especially information security related policies, are often ignored if they might impact quick and simple implementation of ICT services (Talbot & Woodward, 2009). Raising policy breaches with management has often resulted in claims that the policy cannot be enforced; or the policy should be re-written. At times policy enforcement is ad hoc and not enforced uniformly across the whole firm.

No Compliance Program

According to Talbot and Woodward (2009) firms do not usually implement compliance checks within the firm. Compliance reporting and metrics are not produced and made available to relevant levels of management. There is no reviewing of compliance to determine if the security controls and policies employed are effective and being used correctly.

No formal non-compliance reporting

There is no formal reporting of policy breaches and non-compliance. Employees are not aware of what their responsibilities are, how they should report issues, and who to report them to(Talbot & Woodward, 2009). Consequently many issues are not referred to the appropriate areas and information security team was often not involved. Numerous issues have eventually come to the attention of the team long after the event and long after any action should or could have been taken.

Apparent inconsistent enforcement across the whole firm

A number of examples exist within the firm where employees are aware of colleagues being dismissed for activities which appear to breach the acceptable use policy. However, similar cases involving management have only resulted in minor disciplinary warnings(Talbot & Woodward, 2009). This apparent ad-hoc and non-consistent enforcement may have a negative effect the overall realisation of good security behaviours.

3.9. From Information Security Awareness to Information Security Culture

Many recent studies have shown that the establishment of an information security culture in the firm is necessary for effective information security (Eloff and Von Solms, 2000; Von Solms, 2000). Through the establishment of such a culture, the employees can become a security asset, instead of being a risk (Von Solms, 2000; Van Niekerk & Von Solms, 2010).

Information security culture would be where the employees of a firm follow the guidelines of the firm voluntarily as part of their second nature (Van Niekerk & Von Solms, 2010). For example, it becomes routine for an employee to back up his or her files on the laptop on the first Monday of every month, because it is part of the culture and everybody automatically does it.

Williams (2009) suggests how security culture could be defined from analysis and extraction of the key points from the definitions and descriptions of security culture presented above. Each of the quadrants in Figure 3.3 represents an area that is integral to the definition of a security culture: response not reaction, responsibility, community of practice and awareness. The two left hand quadrants represent those aspects that are essential to a security culture and should drive its formation, and the two right hand side quadrants are aspects that should only influence it and are therefore labeled discretionary.

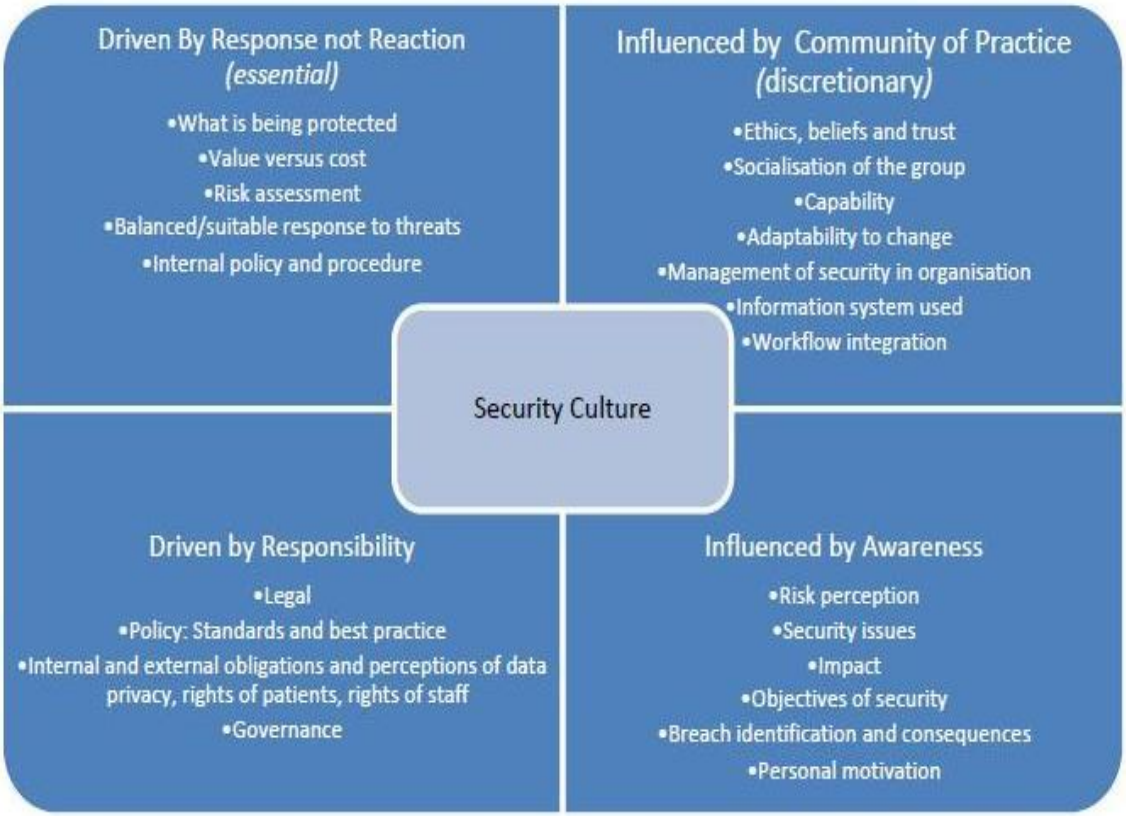


Figure 3.3: Ideal Distribution of Factors Driving and Influencing the Promotion of Security Culture (Williams, 2009).

A summary of how information security awareness ultimately turns to positive information security culture is shown in Figure 3.4.

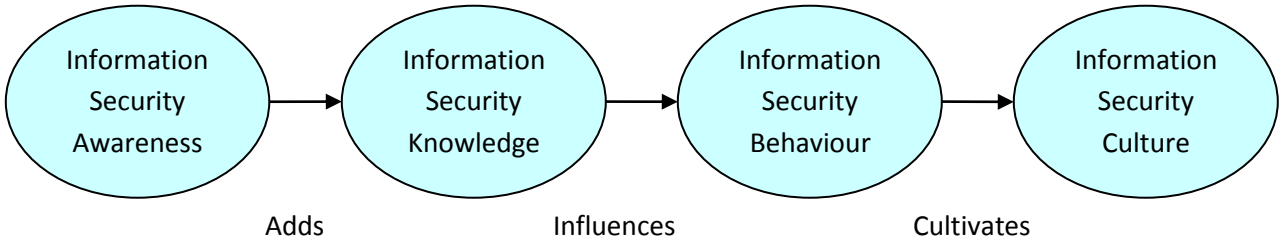


Figure 3.4: The Transition from Information Security Awareness to Information Security Culture

3.9.1. Information Security Culture

There is a little agreement on information security culture definition or what exactly constitutes security culture (Ruighaver, et al., 2007). However Allen (2005) defines culture as shared values, goals and behaviours of a community or group (Allen, 2005). Schein (1999) suggests that culture is a collective phenomenon that grows and changes over time and, to some extent; it can be influenced or even designed by management. In the use and application of information systems culture is a frequently overlooked component of success and failure (Hoffman & Klepper, 2000). Achieving a culture of security will not occur unless employees (as the operational level of security and thus the human factor in the equation) can be convinced of its importance to their daily work and private life. Responsibility lay with each employee to be aware of the security risks that exist in their workplace and the appropriate measures that should be taken. This has become a focus at a national and international level with governments round the world recognizing and promoting its importance by developing their own initiatives (Williams, 2009).

Information security culture should be inter-weaven into the corporate culture. The corporate culture has different levels that can be identified and defined by Schein's (1999) Three Levels of Corporate Culture:

1. The first and most easily observed level of corporate culture is that of artifacts. Artifacts can be described as observed concrete or tangible behaviour, or what an individual can see, hear and feel as they observe a firm. However, it is

important to note that a firm's corporate culture cannot be evaluated and determined by simply observing its artifacts.

2. The second level of corporate culture is the espoused values, which refer to those values that a firm is said to be advocating or promoting (e.g. as outlined in its policies). After a comparison of the behaviour of employees and the firm's espoused values, contradictions may be observed. What these contradictions indicate is that a deeper level of culture is driving the tangible behaviour at the artifacts level.
3. The deepest level of corporate culture is that of the shared tacit assumptions. These are implicit assumptions that are shared by a group of people and encompass the underlying thoughts and values that the employees of a firm believe to be true. This level of corporate culture directly influences the behaviour of employees that can be observed at the artifacts level.

Having identified a variety of potential influences over employee behaviour, it is relevant to consider what the resulting behaviour might look like in a security context. Specifically, this can be seen in the extent to which security practices have been accepted as part of employees' natural behaviour. Table 3.2 compares levels of security compliance and corporate culture levels.

	Artifacts Level (Adhering to correct Information Security Behaviour?)	Espoused Values (Espouse correct Information Security Knowledge?)	Shared Tacit Assumptions (Holds correct Information Security Beliefs?)
Culture	✓	✓	✓
Commitment	✓	✓	X
Obedience	✓	X	X
Awareness	X	X	X
Ignorance	X	X	X
Apathy	X	✓	X
Resistance	X	✓	X
Disobedience	X	✓	X

Table 3.2: Comparing Levels of Security Compliance to the Levels of Corporate Culture (Furnell, 2009)

Security culture should support all organisational activities in a way that information security becomes a natural aspect in the daily activities of every employee (Schlienge & Teufel, 2002). Security cultures assist the enforcement of information security policies and practices to the firm. As a result, each firms goal's is to be able achieve an effective information security culture in their firm. Information security culture will emerge over time and become evident in the behaviour and activities of the workforce (da Veiga, Martins, & Eloff, 2007).

However, organisational culture may have a substantial influence on the security of information, and this could be negative or positive (Chang, & Lin, 2007). It is imperative that the organisational culture reflects a positive attitude on information security in the entire firm (Schlienger & Teufel, 2003; Zakaria, Jarupunphol, & Gani, 2003; Vroom, R. Von Solms, 2004) and it is also important that organisational activities are consistent with good information security culture practices (Van Niekerk, and Von Solms, 2005). On the other hand, (Chia, Maynard, and Ruighaver, 2002), argue on the importance for firms to assess their security culture, and firms management must focus to establish security culture within the firms culture (Ruighaver, Maynard, & Chang, 2007).

Stewart (2005) advocates that security culture should align with business strategy and be incorporated into the firm's corporate culture. Further, it should encourage employees to be alert for potential security issues and raising awareness is key to this strategy. As with corporate culture, if the promotion of a security culture is not given obvious and clear management support, it will fail. This requires that both employees and management are informed and educated on the issues in security and that the management is made aware of breaches in security. The presentation of a business case backed up by financial models will also promote management support (Williams, 2009).

Table 3.3 and figure 3.5 illustrate the stages between the extremes: information security compliance and non-compliance.

Compliance	Culture	The ideal state, in which security is implicitly part of the user's natural behaviour.
	Commitment	Security is not a natural part of behaviour, but if provided with appropriate guidance/leadership then users accept the need for it and make an associated effort.
	Obedience	Users may not buy into the principles, but can be made to comply via appropriate authority (i.e. implying a greater level of enforcement than simply providing guidance).
	Awareness	Users are aware of their role in information security, but are not necessarily fully complying with the associated practices or behaviour as yet.
Non-compliance	Ignorance	Users remain unaware of security issues and so may introduce inadvertent adverse effects.
	Apathy	Users are aware of their role in protecting information assets, but are not motivated to adhere to good information security practices.
	Resistance	Users passively work against security, opposing those practices they do not agree with
	Disobedience	Users actively work against security, with insider abusers intentionally breaking the rules and circumventing controls.

Table 3.3: Levels of Security Compliance Based Upon Individual Behaviours (Furnell, 2009)

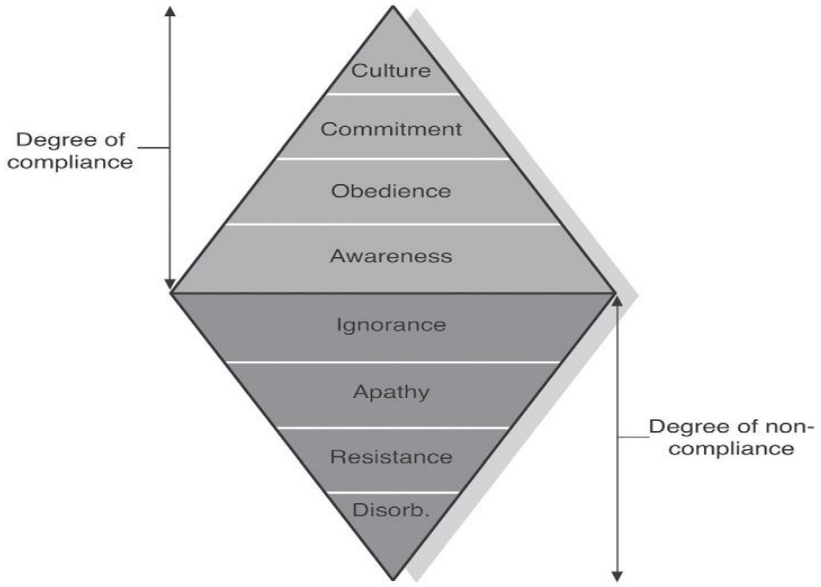


Table 3.4: Levels of security compliance within a firm (Furnell & Rajendran, 2012)

3.9.2. Problems with Creating Culture in Engineering SMEs.

Aspects of security are considered fundamental to those with a certain level of security awareness and obvious to those in the security professions (such as keeping anti-virus data files up to date and continually active, and the secrecy of authentication codes and passwords), are the basis of a culture of security. Such basic aspects become intuitive and automatic in an established security culture. However, there are barriers to this establishment. In Engineering SMEs the problem of creating a security culture includes:

- Reluctance by firms to invest in non-technological solutions i.e. employee training;
- Lack of control over third parties;
- Limited resources and expertise (doing more with less); and
- Lack of appropriate security knowledge.

Whilst in Engineering SMEs it is easier to direct employees to follow policy and procedure because the levels of management are generally fewer and communication is usually more direct (Von Solms & Von Solms, 2004), it can still be problematic to establish a balance between monitoring, control and responsibility. As Chia, Maynard and Ruighaver (2002) report it is difficult to promote a culture of security when there is a lack of management and financial support to improve the security position in a firm. When it is paid lip service as important but neither time nor resources are allocated to address it, security is not perceived as important or something to be adopted intrinsically into daily work practice. This is not necessarily due to a lack of concern rather a lack of recognition of the importance of security and its consequences. Further, there is little doubt that small firms are significantly impacted by the information systems they use and the constraints they are operationally under. This creates more challenges in maintaining privacy and confidentiality of the information they are responsible for.

3.10. Cost of an Information Security Awareness Program

Firms are not able to do business without access to their information resources. However, protecting these information resources often has no direct return on investment. Securing information resources does not as a rule generate income for the firm (Williams, 2009). Business people are therefore rarely interested in how their information resources are protected. From a business perspective, any solution would be adequate as long as it is cost-effective and takes into account issues such as productivity and ease of use. It can thus be argued that the goal of securing information is, to a certain extent, in conflict with the normal business goals of maximizing productivity and minimizing cost. Security is often seen as detrimental to business goals because it makes systems less usable. According to Wood (2005) the only absolutely

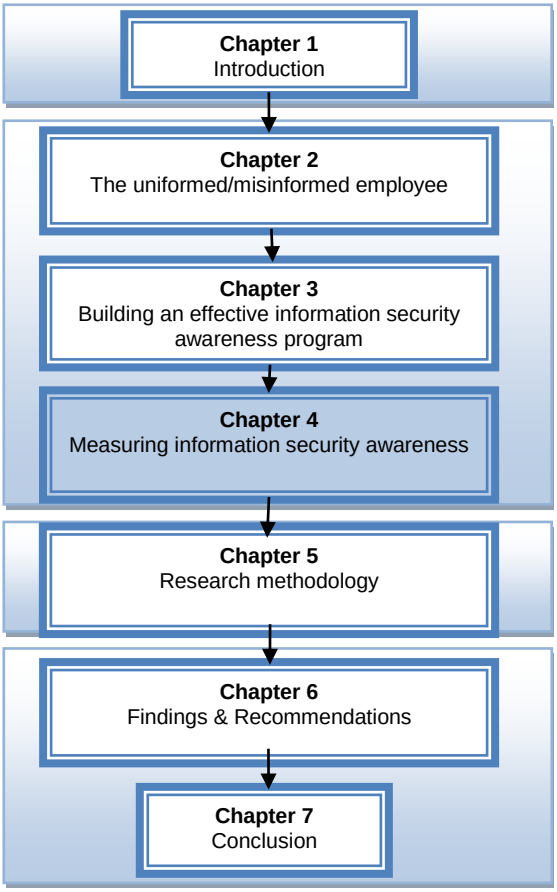
secure system is an unusable one. It is equally unfortunate that a firm's biggest threat to privacy and security are their own staff (BBC News, 2008; Doherty & Fulford, 2005, Williams, 2009). However literature reveals that when a firm implements information security for the first time, the largest portion of the information security budget should be channeled to designing and implementation of an information security awareness program (Voss, 2001), but in many instances, budgetary requirements for security awareness and education are not top priority.

3.11. Conclusion

The more lines of defense a firm has in place, the less likely there will be a successful penetration, additionally there is a better chance that an attack can be detected and the more likely an attacker will give up and move chance on to another more vulnerable target. In this light, many might think of multiple layers of technology such as firewalls, network intrusion detection systems, bastion hosts, etc. that would comprise this defense of depth. However, based on published surveys and analyses, the biggest threat to the information environment is often the employees, hence the employees should be made the firms first line of defense by equipping them with the required knowledge through information security awareness campaigns.

In conclusion this chapter discussed how to ensure a trusted information security conscious environment in a firm. The objective was to show how awareness and training programs lead from ‘‘become aware’’ to ‘‘stay aware’’ and ends up in ‘‘be aware’’, which changes a security culture definitively. The following Chapter will focus on measuring and monitoring change in security behaviours as a result of revised or repeated security awareness campaigns

CHAPTER 4 - MEASURING INFORMATION SECURITY AWARENESS



Chapter 4:

4.1. Introduction

The need for running information security awareness campaigns have been discussed in the preceding chapters. However, how does a firm realise that it actually needs to raise awareness and how does it realise which topics need to be communicated. If the main aim of information security awareness campaigns is to raise security awareness within the firm,the next question in mind will then be “how will the firm know they have achieved that? This problem shows the need to measure the effectiveness of the awareness training. In the previous chapter information security training objectives were established, these objectives where to increase security knowledge so as to cultivate positive security attitude and behaviour. These are the parameters against which the awareness training is to be measured. Awareness measurement is not looking for a tick in the regulatory box in order to provide evidence that everyone in the firm has been

through a security awareness ‘sheep dip’ but to check if it has brought about meaningful and positive behavioural change amongst employees.

Without measurement, it is impossible to establish whether or not an appropriate return on the investment has been realised. Measurement also plays an important part in allowing firms identify aspects where in-depth training is required. It also identifies aspects where it may be possible to spend less without impacting the security risk profile adversely. Hinson (2006) argues that a firm’s management cannot manage what it cannot measure and it cannot improve on what it cannot manage. This makes measuring of information security awareness important for its management and improvements. Measuring also helps to assist in setting up targets and deadlines.

This chapter firstly gives an overview of frameworks used for evaluating information security awareness campaigns. Secondly it identifies what should be measured and how it. Finally a methodology for data analysis is discussed.

4.2. Measuring Information Security Awareness

Different firms adopt different methods of assessing the effectiveness of information security awareness activities. These include both quantitative and qualitative approaches. In general, ENISA (2007) identifies four main approaches, each with different performance indicators:

4.2.1. Process Improvement

This approach assesses the effectiveness of an awareness campaign by looking at its activities i.e. the measures around effort put into the campaign; it does not directly measure whether the end result has improved security. Possible performance indicators include:

- The extent of development of security guidelines. For example, employees can assess how well security guidelines address the main security risks or technology platforms;

- The extent to which the guidance is disseminated. Typical metrics are 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 it is updated; and
- The effectiveness of the deployment of the security guidelines. Surveys that ask employees whether they are aware of guidelines and know what procedures to follow are one way to measure this.

The advantage of process improvement measures is that they are easy to define and to gather. The disadvantage is that they provide only indirect comfort as to whether the program is making the firm any more secure.

4.2.2. Attack Resistance

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

- The extent to which employees recognize attacks. This normally 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 phoning up to ask employees for their passwords, are helpful there.

The advantage of attack resistance measures is that they provide some direct evidence of the actual state of employee awareness. They tend to be good for impressing senior management on the need for investment in security awareness.

The main disadvantage is that there are potentially many attack scenarios; any individual measure will be quite specific to the scenario it is testing. Simulated tests can also be relatively expensive to set up. A risk-based approach can help overcome these issues.

4.2.3. Efficiency and Effectiveness

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

- The extent of security incidents arising from human behaviour. Typical metrics include the number and cost of those incidents. Some firms also consider the proportion of security incidents arising from human behaviour;
- The extent of downtime arising from human behaviour. This is a particular concern in sectors where availability of systems is critical; and
- The extent to which human behaviour caused the firm's most severe incidents. Root cause analysis into serious incidents provides this data; the measure is normally then expressed as a proportion of the total number of serious incidents.

The advantage of these measurements is twofold: firstly, the data can be gathered through the overall security incident monitoring that most information security groups do anyway; secondly, these statistics are usually of great interest to senior management. The disadvantage is that they do not necessarily give a true reflection of security awareness. It is not just security awareness that determines whether incidents occur; the extent to which attacks actually occur is the main factor. In the long term, the trend can be a good indicator of awareness. In practice, however, people often take action based on individual incidents; this may not be the most effective approach.

4.2.4. Internal Protections

This category is concerned with how well 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 can be measured by reviewing a sample of business cases and requirements specifications;
- The extent to which employees protect their data files. Scanning tools can be used to build up a picture of this;

- The extent to which employees have allowed their systems to be infected by viruses or other malicious software. Normally anti-virus activities can 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 can quickly measure this.

The advantage of these measures is that they provide direct evidence of employee behaviours. They assess whether awareness is making the firm more secure and avoid hypotheses or extrapolation. In addition, existing audits (by internal or external auditors) may provide feedback here, effectively for free.

The disadvantage is that any individual measure is quite specific to the behaviour it is measuring. Often, an awareness campaign aims to change many behaviours. This can result in many potential metrics. Each, in turn, may require investment in scanning tools or audits. A risk based or rotational approach can help reduce the ongoing cost.

Most firms use a combination of the four approaches. Blending different measurements enables them to build up a balanced awareness measurement. Decisions are based on the overall picture, rather than on any single measure. Retaining or increasing information security resources requires justifying quantification of the awareness campaign. This research will interrogate mainly the internal protection.

Measuring the effectiveness of various efforts can be costly and time consuming, but it must be done to ensure that the information is reaching the employees (Hornat, 2007). According to a survey by Richardson (2008), 32% of the respondents do not measure information awareness in their firms. This is because of the cost and the absence of commonly agreed and understood standard measurement of the effectiveness of information security awareness and training. Measuring education and awareness is not always straightforward so creativity is vital (Russell, 2002). Whilst Hinson (2006) argues that it is possible to successfully measure information security, he also acknowledges the difficulties inherent in the measurement process. He cautions against measuring the

wrong elements, subjectivity, absolute measurements, the cost of measuring to firms, the interdependencies between management and measurement, measuring process outcomes and the meaning of numbers.

4.2.5. What to Measure

For internal protection, deciding what to measure and how to measure it can be extremely problematic for information security professionals. Literature review however reveals that a number of measures can be effective in providing insight into levels of information security awareness within firms, as well as showing progress when collated on an on-going basis over a period of time. Effective measurement of awareness will involve measuring both operational and performance aspects.

4.2.5.1. Operational Measures- A Useful Starting Point

For many firms, 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

Many firms are using the classroom style of teaching as a primary training tool and this lends itself very well to operational reporting. Typically, the learning style provides a range of reports showing completion rates, assessment scores etc. Usually some level of profiling by department, geography or other specific criteria is possible. This level of operational reporting can be particularly useful for regulatory compliance or internal or external auditing purposes. Whilst measuring the kind of quantitative data described above over a given period is a useful starting point, which will give an indication of trends in levels of information security awareness, it is not necessarily an indication of the effectiveness of training, which is impacted by many different internal and external factors. Nevertheless, it allows drawing up of meaningful conclusions about the impact of awareness initiatives. At the very least, the audience group is understood and the effectiveness of the awareness tools used is learnt. When collated year-on-year, this data can provide a useful internal benchmark showing the growing reach of awareness

initiatives. However to gain a more valuable insight into the penetration of information security throughout a firm, it needs to be combined with qualitative performance data.

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

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

In deciding what performance metrics to capture, it is important to consider the key determinants of security behaviour. Kruger and Kearney (Kruger & Kearney, 2006) highlight three dimensions that should be measured namely what a person knows (knowledge); how they feel about the topic (attitude); and what they do (behaviour). Employees' attitudes towards information security are 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. Attitudes tell us a lot about an employee's disposition to act. Knowledge is important because even if a user believes security is important, he or she cannot carry that intention into action without the necessary knowledge and understanding. Finally, no matter what individuals believe or know about information security, they will not impact security positively unless they behave in a secure fashion.

Enhanced Information security therefore lies in the overlap of attitudes, knowledge and behaviour as represented in Figure 4.1. Consequently, these are the aspects that should be addressed in awareness campaigns and also the aspects that should be measured to evaluate if awareness and training are having the desired effects (Kruger & Kearney, 2006).

Figure 4.1: Enhanced Security

4.2.6. How to Measure

Quantitative research methods such as conducting surveys and the validation of frameworks and questionnaires have been deployed with great success in the information security discipline (Schlienger and Teufel, 2005; Straub et al., 2004; Straub, 1990; Siponen et al., 2007; Woon et al., 2005). Figure 4.2 shows various evaluation and feedback mechanisms that can be used to update the awareness and training program plan

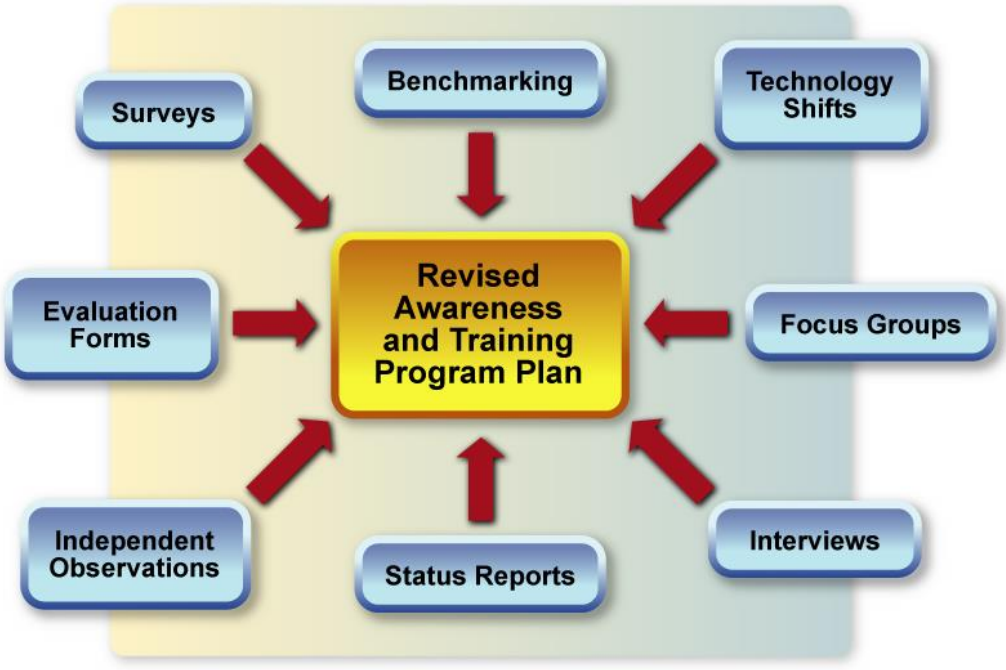


Figure 4.2: Evaluation and Feedback Techniques (Wilson & Hash, 2003)

Literature has shown that measuring such performance intangibles as attitudes, knowledge and behaviour is difficult; however, there are a number of methods which can be used to effectively measure them. The most effective methods are assessment tests, surveys and interviews.

4.2.6.1.Tools for Measuring Attitudes

Surveys (Questionnaires) are the best tools for eliciting information from large numbers of respondents; in addition they enable the identification of broad trends (Hofstee, 2006). A typical way of approaching this would be to use an agreement scale to allow the employees to indicate degrees of agreement with statements about 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 firms can use to study information security behavioural content in general, and attitude and opinions (Berry & Houston, 1993) of employees towards 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 ((Berry & Houston, 1993; Dillon et al., 1993; Furnham & Gunter, 1993)) in DaViega, 2010).

Interviews are ideal for collecting qualitative data. Through a series of open-ended questions, they allow the employee 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).

4.2.6.1. Measuring Knowledge

The most reliable measure of employees' knowledge is a well-designed *assessment test*(Kruger & Kearney, 2006). Many assessment tests are poorly constructed and whilst 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, this helps to validate if employees understand the security behaviours that is required of them (Kruger & Kearney, 2006).

4.2.6.2. Measuring Behaviour

Meaningful indications of employee behaviour or intended behaviour can be captured from *survey* data. Behaviour in surveys tends to be a reasonable indicator of actual behaviour (Kruger & Kearney, 2006). An example of a question which would be a strong indicator of behaviour or intended behaviour is: I would never share my password with a colleague.

4.3. Data Analysis

Kruger and Kearney (2006) proposed using weighting for the data analysis. The methodology used for analysing the data acquired through the measuring methods discussed prior was scaled according to importance as shown on Table 4.1.

Dimensions	Weighting (%)
Knowledge	30
Attitude	20
Behaviour	50

Table 4.1: Awareness Importance Scale (Kruger and Kearney, 2006)

According to Kruger and Kearney (2006) results and importance weights were processed in a spreadsheet application and output is finally presented in the form of graphs and awareness maps. Table4.2 below shows the scale they use to explain the level of awareness:

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

Table 4.2: Awareness Level Measurement (Kruger and Kearney, 2006)

A primary responsibility of information security programs is to raise user awareness of information security issues. A rudimentary training program should minimally educate employees on critical issues. Measuring its effectiveness provides the opportunity to ensure that employees are getting the relevant information they need to do their jobs

safely and effectively. The surveys assess 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 feel passwords don't need to be changed, then they might be need to emphasize on good password behaviour in the information security awareness program. Similarly, if they are asked on appropriate methods for transmitting confidential information to a business partner and 50% of the employees feel that unencrypted e-mail gets the job done, it’s a sign of a deficiency that needs correcting. High scores indicate an effective education program. If employees consistently make errors in the same areas, the awareness is not addressing the correct aspects.

In large organizations it is important to conduct these surveys using a random sample of employees. Random number generators maybe used to select employees from the company directory. This will be to avoid those who play an active role in the firm’s information security program from biasing the results. For best cooperation, employees should be assured that the survey is being conducted anonymously across the firm for potentially adding resources to improve security awareness. Making them feel like they're being graded on a test or that their scores will be reported to management should be avoided as that's a surefire way to drive participation rate into the ground.

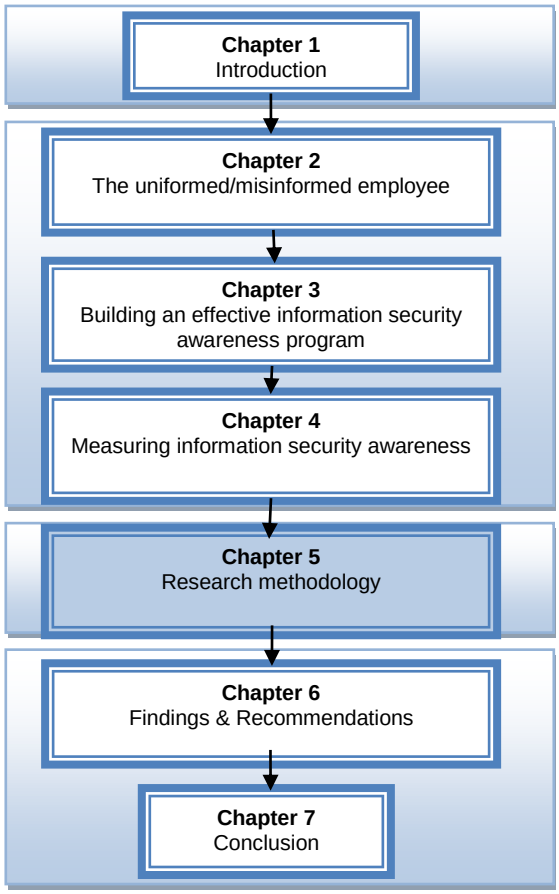
4.4. Conclusion

By its very nature, information security awareness is an aspect that is very critical, this chapter highlighted tools and methods that make it possible to measure the effectiveness of information security awareness training thereby enabling a firm to evaluate whether or not a positive change in the knowledge, attitudes and behaviours of employees has been achieved by their information security awareness campaigns. 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 met.

After developing an assessment instrument for assessing the information security culture in a firm, the results acquired aid in validating the information security culture component categories and ensuring a valid and reliable information security culture assessment instrument. Corrective action plans can be deployed to ultimately help to minimise the threat that human behaviour poses to the protection of information assets.

Quantifying the success of information security efforts can lead to additional resources. At the very least, it can help design measurable information security objectives when budgeting time comes around. Having reviewed literature in Chapter 2, 3 and 4 the next chapter discusses the research methodology followed for this study.

CHAPTER 5 - RESEARCH METHODOLOGY



Chapter 5:

5.1. Introduction

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

Several organisational researchers argue that bringing in knowledge through processes that involve all employees is both necessary and efficient in order to attain all kinds of organizational change (Ehn, 1992; Greenberg, 1975; Greenwood and Levin, 1998; Levin and Klev, 2002). This argument is the theoretical foundation for this chapter. It emphasises on the aspects that affect employees behavioural intentions, the importance of employee participation, plenary reflections and group for improving employees'

information security awareness and behaviour (Albrechtsen, 2010). For employees to play an effective role in the information security of a firm they need to be educated on the importance of their role in protecting information assets and they need to know how to behave in order to fulfill this role.

This chapter details the research methodology followed for this study. First, the proposed information security process, behavioural model and theories underlying the model are discussed. Secondly, motivation is provided for the use of action research as the research design for this study. Thereafter the research paradigm and the method (consisting of background information, participants, the data collection techniques used and the data analysis techniques used) are discussed. A critique of this research study research methodology follows. Finally, the quality issues and ethical considerations ensuring all aspects of the case have been considered.This chapter can be summarised by figure 5.1.

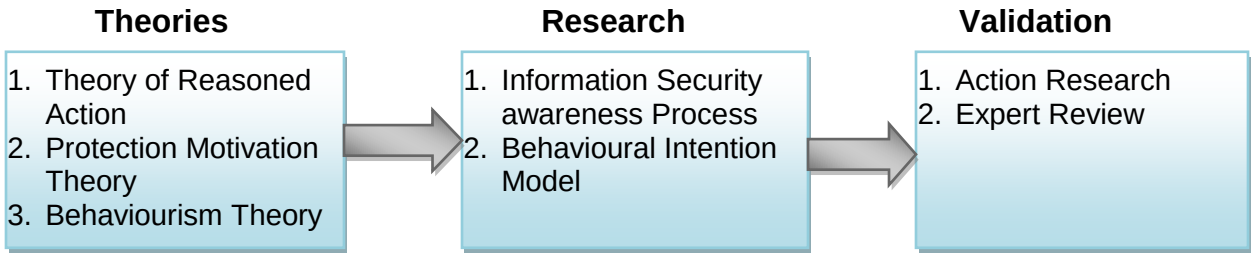


Figure 5.1: Methodology Summary

Exploring a theory-based training program that aims at changing employee behaviour corresponds to a typical aim of action research: finding solutions to the concrete problems in practice (Argyris, Putnam & McLain Smith 1985). Action research aims at promoting simultaneously both the theoretical conceptualisation and practical command of the phenomena of the study. Action research aims to help examine theories and concepts critically in the light of action, and changing ways of working. Hence, this study regards action research as an appropriate approach for the practical evaluation of information security awareness process that aims at firm-wide behavioural changes.

Although action research is typically considered as an interpretive research approach, positivistic empirical indicators can also be used (Hofstee, 2006). They include measurable indicators of employees' improved security behaviour such as decreased number of virus infections. However, as behavioural changes are not always easy to measure, interpretive methods to gather research data are also applicable. One possibility is to interview employees in order to find out whether training has had any impact on their motivation, attitudes, and behaviour. Another method is to use surveys utilising a likert-scale (e.g., five-point continuum from strongly disagree to strongly agree).

The action research was conducted at a civil engineering firm in East London (South Africa). Since security is a sensitive subject its identity has been disguised, henceforth it will be referred to as CEF. This chapter is laid out as follows, firstly the proposed information security process is discussed, secondly the behavioural intention model is discussed and finally the information security measuring methodology is discussed.

5.2. The Information Security Awareness Process

There are two types of awareness processes that can be implemented by firms, that is firm-specific and the generic approach. The generic is the one size fits all type of approach. A firm-specific approach is when an awareness program is based on the information security policies of that specific firm (Du Plessis & Von Solms, 2002). Since goals of firms are different it would follow that policies, and therefore awareness programs that stem from these policies, will also be different for different firms. This means that awareness programs need to be developed to meet specific organisational needs every time.

The proposed information security awareness process is illustrated in the form of a flow chart in figure 5.2. The process starts by checking the existence of an Information Security Policy (ISP); and then verifies whether it is up to date. However, for the purposes of this study it is assumed that a sound and up to date policy that accurately reflects its overall posture towards information security exists. Hence the step of drafting/updating an Information Security Policy (ISP) is beyond the scope of the

research. Figure 5.2 shows the proposed information security awareness process for Engineering SMEs.

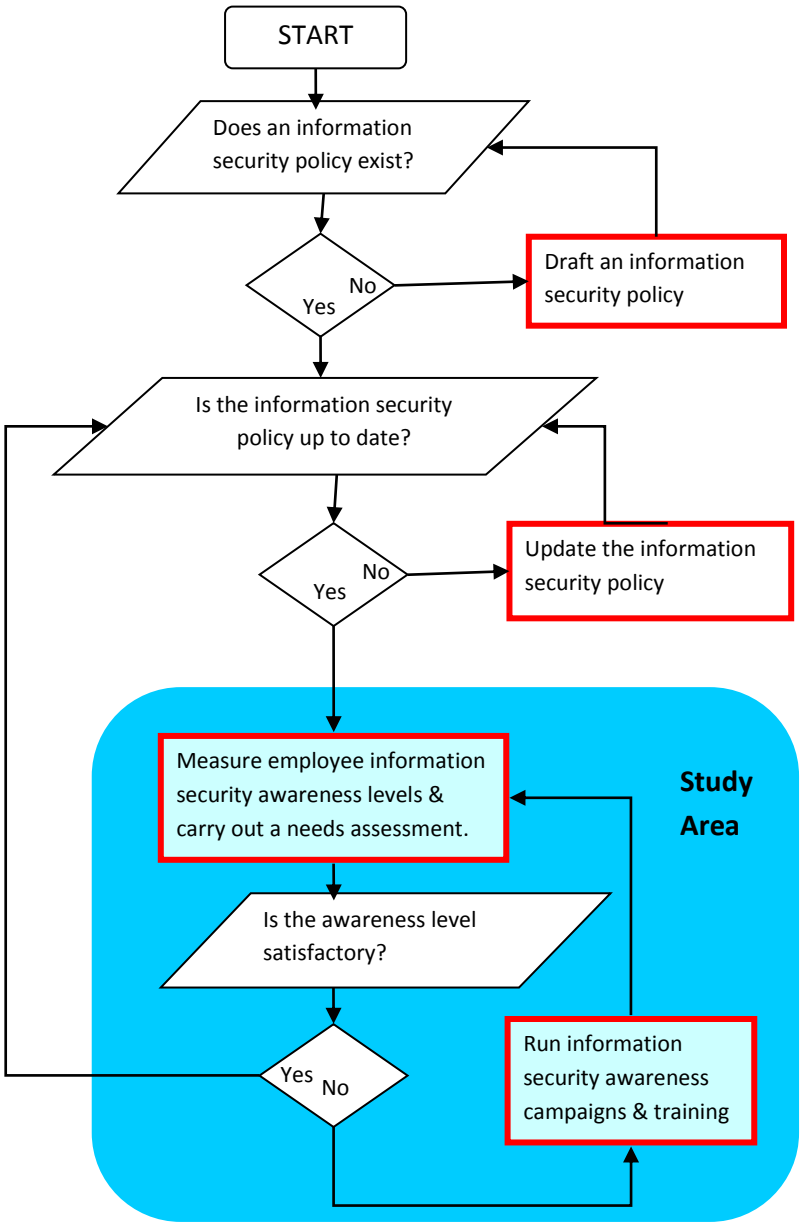


Figure 5.2: Information Security Awareness Process

The next step is to measure employees' current level of the information security understanding so as to expose any knowledge gaps. This needs assessment process highlights current awareness and training needs. Examples of needs that can be revealed by measuring are employees might not have adequate understanding of

password creation, safe Internet usage, viruses and firewalls. This highlights some topics for awareness training. The results also help justify to the 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 (2006) previous research discussed in chapter 4.

The awareness level should be measured again after the awareness campaigns and results will show the knowledge gaps that might still exist. The prior results should always be compared with the current results to monitor if there are any changes. The measuring and awareness campaigns will carry on in iterations until results are satisfactory. The number of iterations will depend on the awareness levels and the intensity of the awareness campaigns. The acceptable information security levels will be stipulated by the firm and this will be discussed in detail later. The study areaof the information security process has two main processes, which are, measuring employee awareness and running information security awareness campaigns. The employee awareness levels are measured using the methods adapted from the model of Kruger and Kearney's (2006). Information security awareness campaigns are based on a proposed Behavioural Intention model to be discussed in detail in the following sections. Figure 5.3 highlights the sections of the proposed information security awareness process that this study will give special attention to.

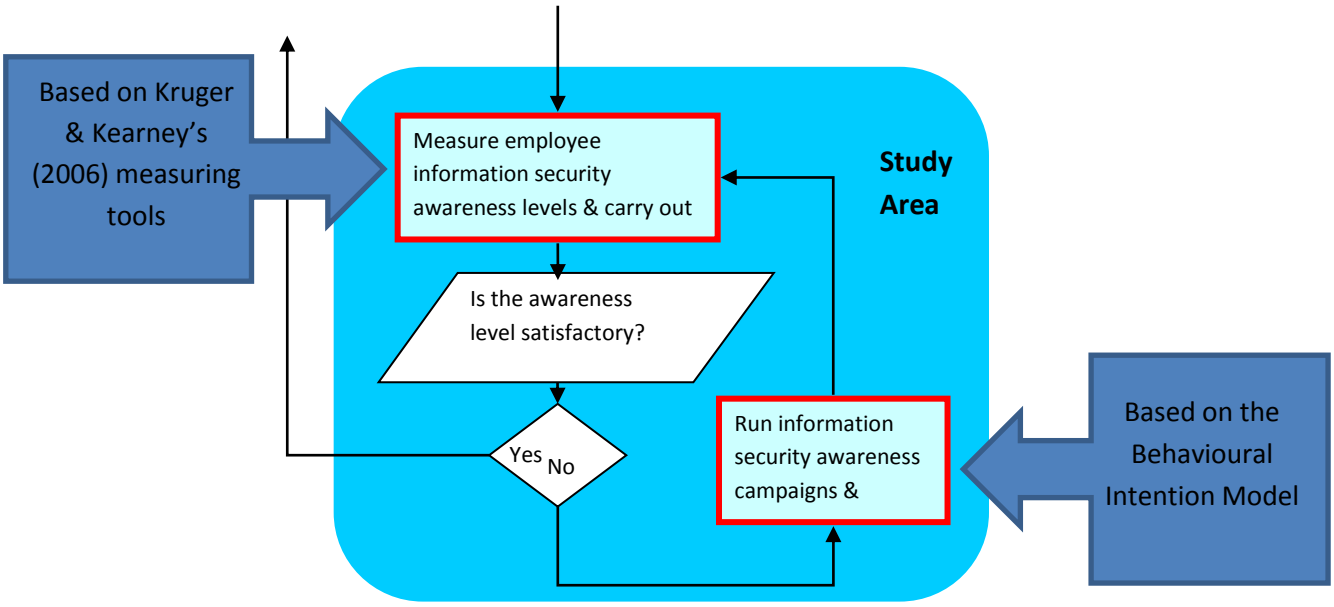


Figure 5.3: Study Area

5.3. The Behavioural Intention Model

Information security theories posit that in order for security efforts to be effective, firms must ensure that employees are part of the security efforts (Da Veiga & Eloff, 2010; Van Van Nierkerk & Von Solms, 2010; Russell, 2002; Schneier, 2008).

5.3.1. Theoretical Background

Based on the problems presented in the preceding chapters, 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 proposed behavioural intention model. Literature has shown that previous works have used research frameworks that integrated TRA, PMT and BT with other theories (e.g. Bulgurcu, 2010; Herath & Rao, 2009; Pahnila et al, 2007). According to Anderson and Agarwal's (2010) review of literature in this area no prior information security research has used all three theories in a single information security study.

5.3.1.1. Theory of Reasoned Action (TRA)

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 a behaviour. 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 favorable 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 (Hale et al, 2003; Miller, 2005; Hogg & Abrahams, 1988).

The Theory of Reasoned Action helps to explain how the employee's attitude towards security and the employee's perceived corporate expectation affects the employee's behaviour towards information security. 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 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 (Lee & Larsen, 2009, Pahnila et al, 2007; Bulgurcu, 2010). 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 security and will aid in communicating the firm's expectations to the employees.

5.3.1.2. Protection Motivation Theory (PMT)

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 (Anderson & Agarwal, 2010). Information security awareness and training instill 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 (Rogers, 1983; Woon et al, 2005). It is composed of the following two items:

(i) Perceived vulnerability i.e. an employee's assessment of the probability of threatening events. In this study, threats resulting from noncompliance with the firm's information security policy (ISP).

(ii) Perceived severity i.e. the severity of the consequences of the event. In this instance, imminent threats to the firm's information security arising 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 (Woon et al, 2005). Coping appraisals are made up of three sub constituents:

(i) 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 sort of skills and measures needed to protect the firm's information asset (Bandura, 1991; Woon et al, 2005; Pahnila et al, 2007).

(ii) Response efficacy: this factor relates to the belief about the perceived benefits of the action taken by the individual (Rogers, 1983). Here, it refers to the compliance with the information security policy as being an effective mechanism for detecting a threat to the firm's information assets.

(iii) 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 have 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 (Lee & Larsen, 2009; Anderson & Agarwal, 2010) as well as Information Security Policy (ISP) compliance (Herath & Rao, 2009; Pahnila et al, 2007).

5.3.1.3. The Behaviourism Theory (BT)

John Watson coined the term "*behaviourism*." Critical of Wundt's emphasis on internal states, Watson urged psychology to focus on obvious measureable behaviours (Skinner, 1965). Watson believed that theorising thoughts, intentions or other subjective experiences was unscientific ((Hull, 1943) in Skinner 1965). Behaviourism as a theory was primarily developed by B. F. Skinner (1965). It loosely encompasses the work of people like Edward Thorndike (1932), Tolman (1951), Guthrie (1952), and Hull (1943) all sited in Skinner (1965).

These investigators had similar underlying assumptions on the processes of learning. These basic assumptions are summarized as follows: First, learning is manifested by a change in behaviour. Second, the environment shapes behaviour. Lastly, 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:*** 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 (Stats &Stats, 1958). 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 of psychologist John B. 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 (Stats &Stats, 1958).

2) ***Operant conditioning:*** there is reinforcement of a behaviour by a reward or punishment. The theory of operant conditioning was developed by B.F. Skinner (1956) and is known as Radical Behaviourism. According to Reynold (1975) 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 (Reynold, 1975). 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 (Reynold, 1975).

5.3.2. The Behavioural Intention Model

Having discussed the theoretical background, this section discusses the Behavioural Intention Model presented in Figure 5.4. It can be observed that all TRA, PMT& BT can be fused to influence desirable behavioural intention. Discussions on the research hypotheses are represented next.

Subjective norms will have a positive effect on ISP compliance behavioural intention. TRA indicates that individuals' attitudes impact behavioural intentions (Ajzen, 1991). To that end, a positive attitude toward ISP compliance bodes well for ISP compliance and 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 will display favourable tendencies towards complying with such rules, requirements and guidelines (Herath & Rao, 2009; Bulgurcu, 2010).

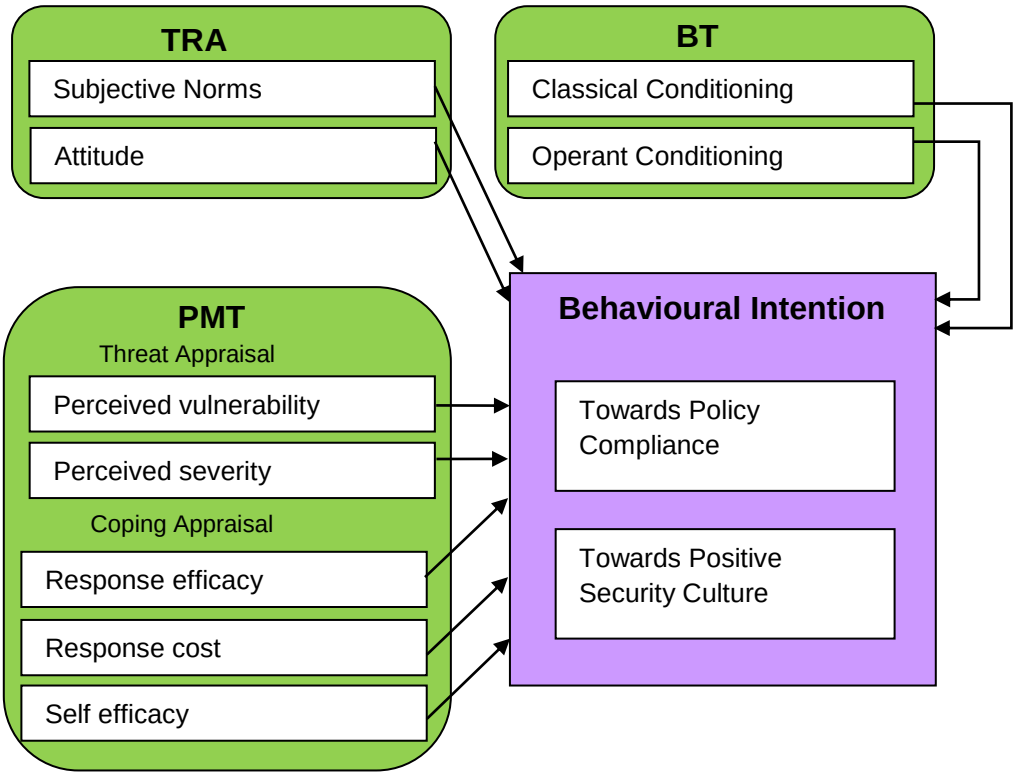


Figure 5.4: Behavioural Intention Model

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 follow organizational ISPs and such individuals may be better placed to realise the threats of noncompliance (Ifinedo, 2012).

Self-efficacy will have a positive effect on ISP compliance behavioural intention. According to Pahnila et al (2007), 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 toward a goal (Milne et al, 2000; Lee & Larsen, 2009). Conversely, if small amounts of resources are required in implementing a measure, it may be adopted Pechmann et al, 2003; Workman et al, 2008). Reducing the Response Cost tends to increase the likelihood of an individual performing a recommended behaviour (Woon et

al, 2005). Past studies have confirmed that Response Costs are negatively related to intention to use security measures (Workman et al, 2008; Lee & Larsen, 2009).

Response cost will have a negative effect on ISP compliance behavioural intention. 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 (Rogers, 1983; Woon et al, 2005; Lee & Larsen, 2009). On the other hand, if the individual has less belief regarding the effectiveness of a measure, he or she may not readily accept it (Rippetoe & Rogers, 1987). Accordingly, individuals who believe that their organization'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 (Herath & Rao, 2009).

Response efficacy will have a positive effect on ISP compliance behavioural intention. In general, when employees perceive a threat, they often adjust their behaviours in response to the amount of risk and determine if they are willing to accept the threat or not (Milne et al, 2000; Workman et al, 2008). Thus, an individual's perceived severity tends to be positively linked to their intentions to follow protective actions (Pechmann et al, 2003). 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 (Bulgurcu, 2010; Pahnila et al, 2007).

Perceived severity will have a positive effect on ISP compliance behavioural intention with respect to safe computing in the firm; however, individuals who view themselves immune to security threats are more likely to ignore security measures at work (Herath &Rao, 2009; Bulgurcu, 2010; Pahnila et al, 2007). On the other hand, it is reasonable to expect that an individual who perceives high vulnerability 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.

5.4. Validation and Verification

The information security awareness process and the behavioural model discussed were verified through expert review by 9 experts in the field. They were then validated through action research. After the action research, 3 more experts reviewed the process and model against the results from the empirical work (action research). The Action research was conducted at CEF and was in three iterations.

5.5. Research Design

According to Hysamen (1994, in Mistry, Minnaar, Patel & Rustin, 2002) a research design is *"the plan or blue print according to which data are to be collected to investigate the research hypotheses or question in the most economical manner."* The researcher has made use of a qualitative research method to gather the empirical data for this study. Qualitative research methods are ideally suited to *"study social and cultural phenomena*" (Myers, 1997) in the social sciences, however, due to the increasing importance of management and organisational issues (above traditional technology issues) in IS research, qualitative research methods are being used more frequently (Myers, 1997). The increased use of qualitative methods can be attributed to the value of an individual's natural ability to talk, and the ability to provide insight into the social and cultural context that is not considered in quantitative methods (Myers, 1997).

Specifically, the researcher employed an action research method for this study of employee information security behaviours. Action Research (AR) is an established research method in use in the social and medical sciences since the mid-twentieth century. Towards the end of the 1990's it began growing in popularity for use in scholarly investigations of information systems (Baskerville, 1999). Action research is an approach to improving education by changing it and learning from the consequences of changes.

Action research is based on change-action and is cyclical in nature. It involves stages of action and research, followed by action. It involves the identification of a problem, collecting information, analysing, planning actions and implementing and monitoring

outcomes. It was originally developed by Lewin (1946) and further developed by Schon (1983), Carr and Kemmis (1986) and Whitehead (1989) all sited in (Baskerville, 1999).

5.5.1. Action Research

Action research (AR) is particularly valuable for its ability to inform theory while making a practical difference. One possible reason for its limited use prior the year 1999 was that the approach suffered from lack of consistent language and lack of guidelines for its conduct and presentation (Avison et al., 1999).

Elden and Chisholm (1993) 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. Thus, Sanford (1970) views action research as a form of problem-centred research that bridges the divide between theory and practice, enabling the researcher to develop applicable knowledge in the problem domain (Peters and Robinson, 1984). Palmer and Jacobson (1971) see action research as a means of using research to promote social action. Further to these descriptions, Rapoport (1970) identifies action research as a form of inquiry that seeks to address both the practical problems of people and the goals of social science within a "mutually acceptable ethical framework" (Susman, 1985).

Considering how action research should be undertaken, Kemmis (1980) notes that it involves the application of tools and methods from the social and behavioural sciences to practical problems with the dual intentions of both improving the practice and contributing to theory and knowledge in the area being studied. Action researchers either participate directly in or intervene in a situation or phenomenon in order to apply a theory and evaluate the value and usefulness of that theory (Checkland, 1981, 1991; Argyris and Schön, 1989; Dick, 1993; Vreede, 1995). Thus action research can be used not only for theory testing, but also theory building and/or expanding (Galliers, 1991).

Eden and Huxham (1996) observe that the intervention of the researcher will often result in changes within the firm studied and will therefore challenge the status quo. They also emphasise that action research must have implications beyond those required for action

in the domain of the project. It must be possible to envisage talking about the theories developed in relation to other situations. Thus it must be clear that the results could inform other contexts.

Some researchers position action research as a subset of case study research (Benbasat et al., 1987; Galliers, 1991), but others (e.g. Vreede, 1995) observe the differences between the two approaches and thus appear to suggest that they should be treated as separate methods. We contend, however, that the three reasons that Benbasat et al. (1987) believe make case study research viable are equally true for action research. The differences between action research and case study are highlighted in Table 5.1 below.

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

Table 5.1: Case Studies vs Action Research (adapted from Vreede, 1995)

Action research usually has the original intention of effecting change whilst pursuing research (Susman and Evered, 1978). The action researcher therefore becomes either a participant or a consultant, though the extent to which s/he is involved varies from case to case. Indeed, there is a continuum between the "describer" of case studies and the "implementer" of action research. In the middle is an "observer" who has social interaction with participants, yet is not a participant in the meeting content (Waddington, 1994). Such a research methodology is strong in the sense that it provides the researcher with an inside and working view of a case. The involvement of the participants in the case also varies from those who get involved with the analysis and reflective learning, to those who prefer only to act.

The action research approach is typically described as a five-phase self-reflective cyclical process as shown in figure 5.5 (Baskerville 1999): (1) problem identification, (2)

action planning, (3) action taking, (4) analysis/evaluation of data, and (5) planning for future action. Furthermore, Kemmis and Wilkinson (1998) state that in addition to this self-reflective spiral, participatory action research has the following key features: (1) it is a social process, because it deliberately sets out to investigate the relationship between the realms of the individual and the social; (2) it is a participatory process, because it encourages people to examine their knowledge and interpretive categories; (3) it is practical and collaborative, because it engages people to examine the acts which link them with others in social interaction; (4) it is emancipatory as it aims to help people to unshackle themselves from irrational, unproductive, unjust and unsatisfying social structures; (5) it is critical in its aim of helping people to recover and release themselves from the constraints embedded e.g., in their model of work; and (6) it is recursive in the aim of helping people to investigate reality in order to change it, and to change reality in order to investigate it.

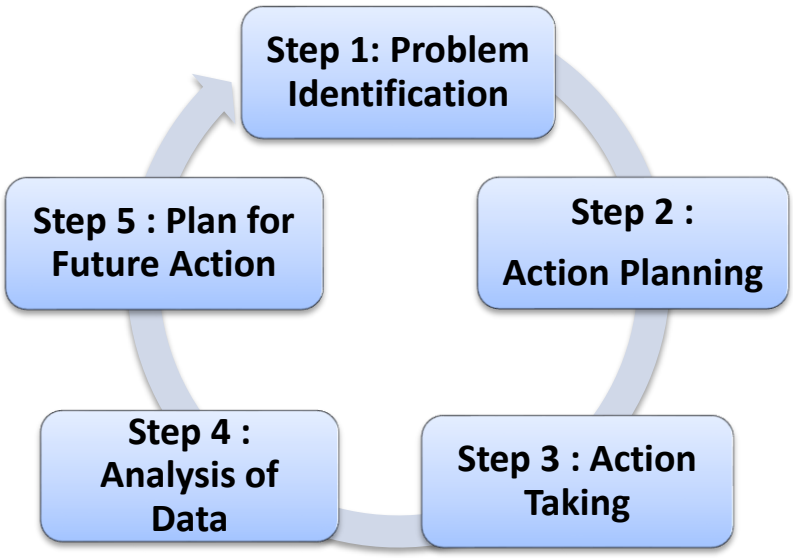


Figure 5.5: Five-Phase Self-Reflective Cyclical Process (Baskerville, 1999)

Step 1: Problem Identification

Diagnosing corresponds to the identification of the primary problems that are the underlying causes of the firm's desire for change. Diagnosing involves self-interpretation of the complex organizational problem, not through reduction and simplification, but rather in a holistic fashion. This diagnosis will develop certain theoretical assumptions

(i.e., a working hypothesis) about the nature of the organization and its problem domain (Baskerville 1999).

Step 2: Action Planning

Researchers and practitioners then collaborate in the next activity, action planning. This activity specifies organizational actions that should relieve or improve these primary problems. The discovery of the planned actions is guided by the theoretical framework, which indicates both some desired future state for the organization, and the changes that would achieve such a state. The plan establishes the target for change and the approach to change (Baskerville 1999).

Step 3: Action Taking

Action taking then implements the planned action. The researchers and practitioners collaborate in the active intervention into the client firm, causing certain changes to be made. Several forms of intervention strategy can be adopted. For example, the intervention might be directive, in which the research "directs" the change, or non-directive, in which the change is sought indirectly. Intervention tactics can also be adopted, such as recruiting intelligent laypersons as change catalysts and pacemakers. The process can draw its steps from social psychology, e.g., engagement, unfreezing, learning and re-framing(Baskerville 1999).

Step 4: Analysis of Data/Evaluating

After the actions are completed, the collaborative researchers and practitioners evaluate the outcomes. Evaluation includes determining whether the theoretical effects of the action were realised, and whether these effects relieved the problems. Where the change was successful, the evaluation must critically question whether the action undertaken, among the myriad routine and non-routine organizational actions, was the sole cause of success. Where the change was unsuccessful, some framework for the next iteration of the action research cycle (including adjusting the hypotheses) should be established (Baskerville 1999).

Evaluation is done by gathering information to answer the research question. Data may be collected from a variety of sources. Using more than one source will increase the credibility of any conclusions. Baskerville (1999) identifies three different methods: breadth, depth, corroboration and there were applied in this study as follows:

Breadth; questionnaire, survey

Depth: interview

Corroboration: observations, checklists, artifacts, videotapes

Step 5: Plan for Future Action

- What will be done differently in the next iteration/ next 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?

The action research intervention at CEF aimed at increasing the level of compliance with the firm's information security policy by finding out and helping to overcome constraints that prevented employees from complying with the policy. As the goal was to achieve firm-wide changes in prevailing practices, it was important to get as many employees as possible involved and committed to the change process. Action research is considered as a suitable research strategy for exploring these kinds of issues. Kemmis and Wilkinson (1998) emphasize that participatory action research aims to help people to investigate reality in order to change it. Hence, due to the nature and goals of this study action research was selected as the research strategy.

When undertaking action research, the researcher started with planning, continued to execute, observe and reflect, before returning to planning a new cycle. The planning itself typically relates to a social or practical problem rather than a theoretical question (Kemmis, 1981). Furthermore, the researcher attached importance to the values, beliefs and intentions of the participants in the study as he attempted to change social reality for the better in an emancipatory frame of reference. Ledford and Mohrman (1993) and Elden and Chisholm (1993) emphasise that participants themselves need to be actively

involved in the research process, sometimes to the extent that they become co-researchers.

The relation with this study's action research is as follows: interested in exploring a hitherto unexplored situation, proposing an information security awareness process that can effect positive behavioural change towards information security by means of e-learning/training, validating and refining the proposed process and model using expert review and action research. It is greatly believed that the refined and tested products are more likely to remain applicable to other similar environments.

5.6. Empirical Exploration at CEF

5.6.1. Background and Participants

Empirical work was carried out at CEF with the aim of determining whether the proposed awareness process and behavioural intention model are actually able to change employee behaviour at the firm and to aid 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 the clients it consults. The action research described in this part of the thesis was conducted with all employees of CEF, twenty eight people altogether and it took place over an ten-month time period from Feb, 2011 to November 2011. The executive of the firm consisted of five people: managing director, structures head, GIS head, resources head, and the water & sanitation head. The firm's technical team consisted of 18 people. Other employees were the office admin personnel.

The Managing Director owns the majority of the company. Additionally, he was the only formally defined manager in the company and as such, responsible for decisions covering most engineering, economic and administrative issues. The technical team was responsible for most design drafting and product development issues. Similarly, the resources head was responsible for human resources, corporate ICT and IS resources and issues.

Action research method is being used increasingly because it is grounded in action, aimed at solving an immediate problem situation and at the same time, informing theory.

Unlike other research methods, where the research seeks to study organizational phenomena but not to change them, the action researchers is concerned with creating organizational change and simultaneously study the processes. Action research is strongly oriented toward collaboration and change involving both the researchers and subjects (Collis & Hussey, 2009).

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

CEF invested considerably on the research and development of the information security process. According to the firm's management, the resulting innovations will go a long way in protecting of their information asset as its company's values include protecting customer and business partners' information. This was the main reason why the management of CEF welcomed the development of a companywide information security campaign. However fortunately this was not done from scratch as an information security policy and end-user instructions were already in place. All employees had signed one on induction although nearly all did not remember they did or the contents of the documents. Hence the researcher assumed very low level of employee awareness of information security issues.

However, on the contrary the firm's executive assumed a relatively high level of employee awareness as it advocates that the employees read and understood the policy when they signed it. They are however puzzled by the high rate of violations of the firm's security policy. This 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 to that still remains a mystery (Personal Communication, Managing Director of CEF, January 2011)."

After some serious discussion with the researcher, the firm's Managing Director was made to realise that the negative security behaviours could be indeed due to lack of information security understanding. This led to the researcher being granted permission to engage with an action research. What was in it for the Managing director? He would have all his employees educated on good security practices and he would get statistics of the awareness levels. What's in it for the researcher? The researcher got to validate, refine and test the information security process and model in a real life scenario. CEF was selected as a host firm for empirical exploration of the information security awareness process and the behavioural intention model because it exhibits characteristics of a typical Engineering SME. The size of the company made it possible to informally interview all employees several times during the research process. This was to allow rich interaction between the employees and the researcher and consequently, to provide detailed information regarding compliance and non-compliance with information security policies and instructions.

5.6.2. Methodological Assumptions

In this action research project, each employee at CEF was considered an active processor of the information he/she receives. Hence, he/she was regarded as able to decide personally whether to comply with the firm's information security instructions, such as the email policy. Additionally, it was noticed that this decision was affected by 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 1989). 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 necessary for achieving the study's goals of increasing the level of compliance with firm's information security policy.

5.6.3. Research Strategy and Position of the Researcher

In this action research, the researcher was not regarded as an objective, passive outsider. The firm's executives, resources head and other employees expected him to be an active participator, planning, designing and delivering the training program and evaluating the results. Consequently, the researcher became responsible for planning and implementing the information security awareness training program. In addition, the researcher acted as a consultant. The researcher's involvement is best described as *expert involvement*, as the researcher was regarded as an expert among the collaborators. Some of the tasks were individual, but cooperation between the researcher and the collaborators was also an essential part of the research process.

5.6.4. Principles of Information Collection and Analysis

Information was collected and analysed constantly throughout the research process. Three methods were used for collecting the research data: (1) informal interviews, (2) online survey, and (3) participatory observation. The goal of the information security awareness training program was to increase employees' compliance with the firm's information security policy. For this reason, information regarding their previous skills, knowledge and behaviour was collected. A survey was used at the beginning of the process for collecting information related to employees' knowledge, attitude and behaviour on information security.

The survey contained questions governing information classification rules, secure use of the Internet and, especially, the secure use of email. The information gathered was used to evaluate whether the employees had the necessary knowledge for complying with the security policy. Informal interviews were also used to gather information governing motivational factors related to compliance with policy. In addition, they were used to collect the information governing the employees' skills and knowledge related to 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 considered using audiotape to record the interviews. This seemed to be the most useful means 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 terms. 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 making them 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 verifications were done during the analysis phase whenever this was perceived necessary to avoid wrong interpretations. According to Stinger (1999), a major problem with interviews is that questions are easily influenced by the researcher's perceptions, perspectives, interests, and agendas. To avoid this, the researcher asked questions that are relatively neutral. This is necessary in order to diminish the extent to which participants' perceptions will be governed by frameworks of meaning unintentionally imposed by the researcher.

The researcher started with grand tour questions that were sufficiently global to enable employees/participants to describe their situation in their own terms. The aim was to give focus without giving direction or suggesting forms or types of responses (e.g., "Tell me about information security in your work."). Other forms of global questions included questions on what is 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 (e.g., typical or specific) that focus on concepts already presented (e.g., "You earlier mentioned that this policy is difficult to comply with"), this is done to gain more detailed information about issues already covered. In all phases of the interview, the researcher took a neutral stance and wrote down the responses as accurately as possible.

Following the approach presented above, all twenty eight employees at CEF were interviewed once or twice during the process. All the interviews were recorded by using field notes. Some of the interviews were conducted with individual employees, but group interviews were also used especially during lunch times when everyone was in the canteen. The information gathered was analysed continuously and the analysis was verified with all participants. The aim was to identify the themes that emerged from the information and whether these themes supported theories concerning compliance with information security instructions. The analysis formed the basis for developing the intervention.

Furthermore, participatory observation concerning the impacts of the intervention was conducted in normal working situations. In addition to the researcher, director and the resources head and other employees observed the results achieved throughout the study. Moreover, the researcher uploaded large amounts of material on the corporate intranet; these included the firm's security manual, security audit reports, memos of meetings, and risk analysis reports.

5.6.5. Conducting Action Research at CEF

The total duration of the study then totalled to 11 months. This eleven-month action research consisted of 4 research cycles. Table 5.2 shows the topics that had major emphasis per iteration, basing on the knowledge gaps.

Needs assessment	• Password construction & Management, • data confidentiality, • email usage	**Iteration 1**	• Viruses, • Firewalls, • physical security, • wireless security
Iteration 2	• Identity theft, • internet usage, • intellectual property	**Iteration 3**	• Encryption, • backups, • home offices

Table 5.2: Major Themes per Iteration

An initial survey (needs assessment) was performed; one month later iteration 2 was conducted. Thereafter the following iterations where spaced by three months this was to allow the employees to start practicing what they had learnt and to allow the researcher to also evaluate the stability of the awareness and behaviour produced.

Once the employees have gone through the online security awareness training, and displayed sufficient information security understanding, they received a certificate to show they completed the requirement as per their Managing director's directive. It was decided that the Security Awareness Training Certificates be only valid for one year, hence the employees have to repeat the process yearly. The questions are however changed yearly so that no one takes the same test twice. Once the certificate is coming upon its expiration date the employee just logs back into the system, reviews the information, and takes the assessment again. Since this is done on a yearly basis most employees said they do not mind having to complete the training and testing process again and we have received favourable responses indicating that the updated information was found to be very useful.

The information security process and behavioural model where reviewed by nine information security experts and this assisted in their verification. The action research was also conducted for verification and validation purposes and that also assisted in their refinement.

5.7. Information Security Awareness and Training

5.7.1. Information Security Awareness and Training

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?" (William, 2002). Unfortunately not everyone does so even when they know better. This highlights that the real challenge is not just to make people aware, 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 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 (Johnson, 2006).

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 campaigning 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 program seeks to explain proper rules of behaviour when using the firm's ICT resources. The program communicates information security policies and procedures that need to be followed. This must precede and impose sanctions when noncompliance occurs (Herath & Rao, 2009).

The BERR (2008) survey suggests that the majority of firms rely upon written materials of some form. 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 (2008) and Ricer et al (2005) reported 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.

An e-learning system was used in this study instead of the conventional classroom style because it provides a configurable infrastructure that integrates learning material,

policies, and services into a single solution to quickly, effectively, and economically create and deliver 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. The next section therefore seeks to explain how e-learning can be used as a tool for communicating and testing information security awareness training.

5.7.2. Implementation Method (E-Learning)

The information security awareness communication path used was E-Learning. E-learning has grown tremendously 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 (Smart & Cappel, 2006). 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 for information security training in Engineering 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 by 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 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 website for training and awareness was constructed as follows (Please refer to Appendix B for a copy of the website):

Home Page: provides an introduction to information security and the motive behind the training/ awareness. Employees needed to be motivated as to why information security is important. The home page then links to the awareness pages.

The Awareness Pages: these supply information on topical issues and examples of breaches. These pages contain all the information security information required by employees.

The Assessment Page: this was used as the data collection tool for acquiring data from the employees which 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 program including the link to the awareness and training website.

After releasing results of the needs assessment, CEF's Managing Director stated that *"I know believe that the employees lack the skills to behave securely. In addition, some employees seem to lack knowledge about the firm's information security rules. Consequently, confidential information is not always recognized. Furthermore, I believe that there are employees who do not understand the risks and the possible consequences poor security practices (Personal Communication, Managing Director of CEF, June 2011)."* On the basis of these considerations, the researcher assumed that CEF's employees needed more skills and knowledge. The managing director, resources head and researcher considered it appropriate to address the above-mentioned shortcomings by running online awareness campaigns.

5.8. Measuring Information Security Awareness

Information for the baseline was gathered from surveys, observations, audits, specific security tests and from help desk reports. After the security awareness campaign was launched, it was important to measure its success and draw conclusions from the measurement 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 was to detect the effectiveness of the message, method, and behavioural intention change.

According to a survey by Richardson (2008), 32% of the respondents to a survey do not measure information awareness in their firms. This is because there are no commonly agreed and understood standard measurements of the effectiveness of information security awareness 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 (Hinson, 2006; Kruger & Kearney, 2006).

5.8.1. What to Measure

Kruger and Kearney (2006) 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.

5.8.2. How to Measure

Measuring such intangibles as Attitudes, Knowledge and Behaviour is difficult. This study makes use of assessment tests for eliciting information from the employees.

Online Surveys (assessment tests) Assessment tests enable identification of broad trends (Hofstee, 2006). An agreement scale was used to allow the employees to indicate degrees of agreement with statements about security.

The assessment test had questions that seek to test for knowledge, attitude and behaviour. The following are examples of the questions that were asked:

Example statement for test of *knowledge*:

Internet access on 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**

5.9. Conclusion

This research methodology chapter was conceived against the backdrop of efforts made by Engineering SMEs to protect their information assets. Firms usually procure technological tools to help them achieve success on business fronts. As an underlying theoretical background in the area, this chapter drew on three relevant persuasive theories which included Behaviourism Theory, Theory of Reasoned Action and Protection Motivation Theory.

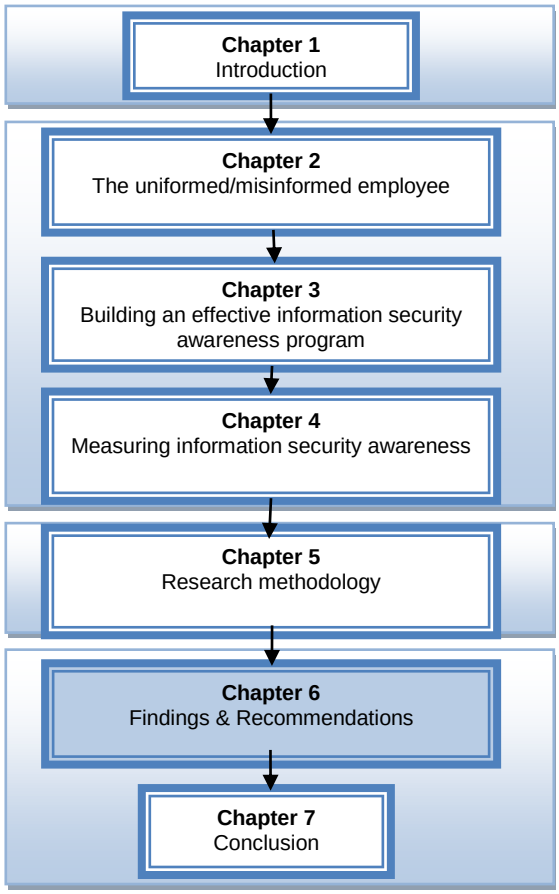
In this chapter a detailed research philosophy was presented, strategy and methodology according to which research was conducted. A substantial literature review, assisted in the enhancement of earlier research models to aid the development of an information security awareness process and a behavioural intention model. Finally the operationalisation of the practical side of the dissertation is detailed. This includes the designing and validation of the information security process and behavioural intention model and detailing broad procedures for data analysis and behavioural change.

Qualitative methods of assessment were used mostly. These included online surveys to measure knowledge retention and random inspections to assess the implementation of workplace security guidelines. Determining from the beginning of awareness program what criteria will measure and how it will be measured allows gauging the success of the awareness efforts. After each iteration the effectiveness of the efforts were measured. This allowed for adjustments on the message focus and method of delivery to obtain the best results for the environment.

In closing, getting employees to know and care about information security was definitely a challenging task. Identifying themes helped craft a cohesive professional awareness website that was clear enough for employees to instantly recognize the message. Determining the concepts employees should understand was a priority, as efforts focused on the topics that lacked but critical to safeguarding the firm's information security asset. Finally, repetition was the key to getting the message across. Security awareness messages were conveyed on a regular basis and in a variety of mediums so that maximum exposure could be achieved.

Having discussed the research methodology a discussion of the findings and recommendations follows in the next chapter.

CHAPTER 6 - FINDINGS AND RECOMMENDATIONS



Chapter 6:

6.1. Introduction

The preceding chapter presented the methods adopted during the research process for this study. It described the research methodology that was used to collect, analyse and apply relevant literature to an identified problem. The study was carried out to firstly discover the vulnerabilities that the uninformed employee exposes the firm to. It then goes on to discuss a process which can be followed when running an information security awareness program. It also discusses a model that helps to explain the human aspects that should be addressed in order to cultivate positive security behaviours. This information security process and behavioural intention model was verified and refined though an expert review process and validated through an action research.

This chapter presents the findings and recommendations that resulted from the action research and expert reviews that were conducted. Firstly this chapter highlights the findings of the research that was conducted and then the expert review process will be explained. Finally, recommendations are given.

6.2. Findings

As detailed in the previous chapter, the action research involved making use of multiple data collection techniques to gather data for this study. These techniques include online surveys, participant observation, informal interviews and document surveys.

First, the findings of the online survey provided background and insight of the information security awareness levels of the firm's employees. Secondly, the participant observation allowed the researcher to gain first-hand experience of employees' behaviour in real life situations. Thirdly, the informal interviews conducted provided details of feelings of the employees towards information security. Lastly document surveys helped to show the occurrence rate of security breaches over the study period

6.2.1. Findings of the Online Survey

The study collected qualitative data through online surveys four times at specified time periods. The first round of data collection was during the needs assessment, and the following times were during iterations 1 to 3 as discussed in the preceding chapter. The information collected was used to measure the information security awareness level of the employees and also to identify knowledge gaps that would need to be addressed in the next information security awareness campaigns and training. The four online surveys had different but similar questions. Although the surveys had different questions, they all had a similar structure as they were measuring the same attributes i.e. knowledge, behaviour and attitude. Please refer to CD-RROM in Appendix B for the survey structures and questions.

The use of qualitative methods is important for studying the dynamics of the intervention, as qualitative research provides understanding of social processes (Strauss and Corbin, 1998; Thagaard, 2002). The aim of the qualitative evaluation of the intervention was to measure the information security awareness levels of the employees, identify knowledge gaps and to assess if the intervention is making any progress in the intended employee behavioural intention moulding. The qualitative data collected through online surveys was analysed by looking for patterns in the data that described how the intervention was interpreted and why the intervention modified or failed to modify awareness and skills. Furthermore, the data was also analysed for reasons for these patterns.

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. 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. Table 6.1 summarises the information security understanding of the employees per iteration.

	Needs assessment	Iteration 1	Iteration 2	Iteration 3
Employees understanding level	6 (21%)	18 (64%)	24 (86%)	27 (96%)

Table 6.1: Employees Information Security Awareness Understanding Results

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 having information security understanding levels of over 50% is not a true reflection of the firms overall information security awareness levels hence Kruger and Kearney's (2006) method of analysing data acquired through the measuring methods discussed in the preceding chapter was adapted. This method involved weighting the three aspects being measured as follows (Table 6.2):

Dimensions	Weighting (%)
Knowledge	30
Attitude	20
Behaviour	50

Table 6.2: Awareness Importance Scale (Kruger & Kearney, 2006)

This weighting was verified with the managing director, IT technician and the resources head of the firm who agreed that behaviour was the most important measure followed by knowledge then lastly attitude. The results and importance weights were processed in a spreadsheet application and the output was finally presented in the form of graphs and awareness maps as was done in Kruger and Kearney's (2006) study. Table 6.3 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.

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

Table 6.3: Awareness Level Measurement (Kruger & Kearney, 2006)

Table 6.4 summarises the results categorised by the knowledge, attitude and behaviour.

	Knowledge (30%)	Attitude (20%)	Behaviour (50%)	Total (100%)
Needs assessment	12	11	22	45% (poor)
Iteration 1	18	12	30	60% (average)
Iteration 2	22	14	35	71% (average)
Iteration 3	25	15	38	78% (good)

Table 6.4: Iteration Results of the Action Research

The 78% awareness level was satisfactory and there was no need for a forth iteration. It was possible to measure the effectiveness of information security awareness training by using the tools and methods outlined by Kruger and Kearney (2006). These enabled the firm to evaluate the extent to which awareness activities have impacted on behaviour, attitude, and knowledge and therefore, whether or not the initial training objectives have been met.

6.2.2. Findings of Participant Observation

Participant observation is fundamental to any action research study. The involvement of the researcher in this type of observation can vary from complete observation to complete involvement (De Vos, et al., 2005). The researcher's participation in this scenario is an equal mix of observation and involvement. The researcher's observations at CEF were concerned with employee behaviour towards information security awareness.

Observations relevant to this study centre on one particular instance – the computer network of the firm went very slow due to a virus. This resulted in major losses as production was very slow for three days and 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 is equipped with an antivirus most employees turned them off as they report they slow their computers and they delete some email attachments. The virus is assumed to have entered the firm's computer network through one of the computers that has antivirus software uninstalled or disabled. It then duplicated itself onto all the other computers and the servers. This slowed down the server intensively such that it took over 25minutes 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 took the whole day for the researcher and the computer technician to get rid of the virus. The antivirus software was also updated and reactivated on all the computer resources. This issue is typical of problems encountered at this firm; which the researcher believes to be intensified by the lack of security knowledge.

Although firewalls and antiviruses are in place, information security awareness and training was necessary in order to get employees to use them correctly. It required collaboration of all employees. The researcher played an advisory role as CEF did not have the necessary skills or knowledge in-house to handle such a problem.

Another observation was that the employees keep their passwords underneath their keyboards or pasted behind their screens. They also share their passwords with their spouses and amongst themselves. On several instances employees come in with their spouses and children and allow them to use the firm's computer resources. Also when an employee is absent from work, colleagues can call the employees to ask for the login credentials so they can login. This is not necessary as their own login credentials will be able to log on to the system.

6.2.3. Findings of the Document Survey

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

The researcher intended to obtain documentation from CEF (the action research study firm) to provide insight into the occurrence's and solutions to information security breaches that the firm has encountered. In particular, the researcher was interested in documented evidence viruses, identity theft, phishing attacks and physical security.
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 this study. The researcher's efforts to find these types of documents proved fruitless.

6.2.4. Findings of the Informal Interviews

Interviewing is the most significant data collection method for research studies and in particular for qualitative research (De Vos, et al., 2005). Kvale 1996 (in De Vos, et al.,

2005) view interviews as an attempt to comprehend participant's point of view and extract meaning from their descriptions of experiences.

Interviews were conducted during the needs assessment and all iterations of the action research. The interviews where to get an idea of the extent of information security knowledge of key employees. The findings from the interviews are discussed below and the findings from the needs assessment online survey helped the researcher to compile a list of topics that the first round of the information security awareness and training needed to address.

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 role they played in the observations discussed above.

Participants were informed of the goal of the research study and provided with background of the field of information security. There were no interview questionnaire as the questions asked were random but field notes were taken. Furthermore, participants were encouraged to discuss other issues relating to these questions that emerged during the assessment test.

6.2.4.1. Respondents of the Informal Interviews

Managing Director

The managing director of CEF is involved in all aspects of the firm. He is aware of every issue that occurs in the admin and technical environment. The nature of the firm and the managing director's role in it requires that he be on hand to assist in obtaining a solution to prevent any stoppages in production. When a problem arises, employees always refer the situation to the managing director in order to figure out the solution.

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 reached. The resources head performs the majority of the problem-solving activities.

Technical employees

The five technical employees chosen to participate in the interviews were two engineers, one CAD operator (draughtsman), one GIS operator and the IT technician. The way problem-solving is dealt with in the current scenario, is they report all IT related problems to the IT Technician. These employees except the IT technician have little responsibility to ensure the problems are resolved.

Administration staff member

The administrative staffs of CEF are not intricately involved in the engineering aspect of the firm, but are rather on the marketing and tendering process. However, due to the small nature of this firm, administrative staffs do play important roles in problem-solving situations related to information security and privacy issues.

Temporary employee

The temporary staff member was recruited temporarily to assist in the implementation of a new civil engineering software package. This employee was only available for 3 months of the research. The employee was only asked questions relating to experiences at CEF.

6.2.4.2. Interview Responses Summary

The questions asked during the interviews were open ended and notes where taken, however there were 10 Questions that were asked randomly at the employees. The responses to these questions are summarised in table 6.5.

Security Policy
1. Does this firm have a formal Information Security Policy in place?
• The temporary employee said he is not sure, the managing director said yes and

the rest said no although they is one in place. • However the human resources have a signed copy of the document for each employee.
2. Do you think you have enough knowledge and skills to make you behave securely when using the firms ICT resources of the firm?
• The respondents generally felt that they have enough information security knowledge and skills. • The admin employee however felt that she would do better with a bit of training.
3. Do you think the firm is doing enough in terms of physical protection of the information asset?
• All participants were happy with the security, they said they have burglar gates, alarm with rapid response and CCTVs are installed in all offices and passages.
4. Do you think the firm is doing enough in terms of technological protection of the information asset? (Firewalls, antivirus, 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 in slowed down their computers. • Majority of them did not check if their antivirus is up to date.
5. Do you think you should be part of the firm's information security initiatives?
• Most participants believe security is complicated and time consuming and that the ICT Technician should be responsible for security not them.
6. Is there any system in place to measure the success of and or compliance with security policy in this firm?
• Most respondents believe the CCTVs in the premises are to spy on them hence they believe compliance is being monitored. • Most of them said compliance is mandatory failure of which can result in disciplinary action.
7. Do you think the information on the server might be of any value to someone other than your firm?
• All answers had something in common, that is they think their competitors would

love to know their cutting edge secret.
8. Have you ever made any mistake that ended up posing as a security threat to the information asset?
• Majority of the answers said they seem to behave securely although one admitted that they once opened a website that had a virus and it was detected by the antivirus.
9. (a) Do you take any information/or laptop home so you can work over weekends/ at night?
• Most responded with no, except for the managing director who said he takes 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 has a password on his laptop in case it is stolen. However the answers from the other participants were irrelevant as they do not take any data or equipment home.
10. Do you sometimes use your work computer for personal things, e.g. internet banking, online shopping, social networks, etc.
• Everyone answered yes, however they say most sites especially social networks are blocked, so they don't use it that much.

Table 6.5: Interview Response Summary

6.3. The Expert Review Process

This section describes the process in which the research project and its main contribution was critically analysed by a number of experts. By following the Delphi Technique, a total number of twelve experts in the field of information security were approached and were requested to conduct a critical analysis on the main contribution of this study. This analysis occurred over four distinct rounds of review, with feedback from each round serving as the refinement of the research contributions analysed in each consecutive round that followed. The details on each round of the review process are as follows:

6.3.1. Expert Review Process: Round 1

In this round, three experts from the Information Security South Africa (ISSA) organisation were approached and requested to review the research project. The response from these reviewers was then summarised and used to further develop and refine the study. The main recommendations and the results obtained from this round were:

- A reviewer 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.
- A reviewer questioned if the model will also change the behaviour of the malicious insider. Thus, in order to remove confusion that may be present, the study highlighted that it will only focus on the uninformed employee although the malicious employee is equally dangerous.
- A reviewer highlighted that the study had included some very old literature references and sources, which made them feel that the problems highlighted could have long been solved. This impacted negatively on the overall credibility of the study. Consequently, these sources were replaced with more up-to-date and credible sources of literature.
- It was pointed out by one of the reviewers that the study lacked focus in certain areas and did not link the risks posed by the employee to lack of knowledge. Literature pointing out the risks of the ignorant insider and statistics were then included.
- Reviewers mentioned also that the Diagram of the information security process was excellent for illustrating the steps to be followed; however, they had some issues with the diagram being unclear and unreadable. The diagram was then redrawn and improved accordingly.

6.3.2. Expert Review Process: Round 2

After the first round was done, the research was updated, and after 12 months a second round of review commenced. Three different experts from Information Security South Africa (ISSA) organisation were asked to assess the study. Their comments and

opinions were then received, summarised and implemented accordingly. The key responses received from these experts consisted of the following:

- A reviewer pointed out that some of the statements made in the research project were worded incorrectly or unsubstantiated, such as the comment “risks posed by the human element cannot be totally eliminated”. This resulted in the research project being refined, removing all claims that were unsubstantiated and correcting the wording to portray the correct meaning of those statements.
- It was also identified that the study needed to emphasise the final contribution it makes, as it lacked the required focus. This led to more discussion on the final contribution of the research project i.e. the information security process and the behavioural intention model. It was made clear that the main contribution of the study is an artifact in the form of a model and a process that can be followed for information security awareness training and campaigns.
- It was also suggested that the study better justifies the underpinning theories. As a result, explanations of why the Theory of Reasoned Action, the Protection Motivation Theory and the Behaviourism Theory were chosen, and related to the research project was added.

6.3.3. Expert Review Process: Round 3

After another 12 months a third round of assessment was conducted, this involved a different set of experts from the ISSA organisation, of which three were consulted to review the research project’s findings. The following were their responses:

- A particular reviewer requested that a better specific definition of an insider should be included in the research project, as the entity was not described correctly and in sufficient detail. For example whether temporary workers or consultants insiders. Thus, a definition specific to this study was formulated.
- All the three reviews agreed that the research flows well but has a poor ending. They said the conclusion of the research study is very weak. Thus, the whole conclusion chapter was revised and expanded upon and a more comprehensive discussion was drafted.

- A reviewer found the topic “Towards an e-learning based information security awareness process” misleading, as the emphasis of the research is rather on the information security process to be followed. The e-learning component in itself is not novel but does serve the purpose of validating the model. As a result, changes were made to the research study topic.
- A reviewer stated that in the study, the notion of awareness and training was introduced but in the majority of the study, the term campaign was used in places that training was more appropriate. The authors were intentionally trying to refer to both concepts of awareness and training, but failed to distinguish between the two correctly. Thus the research project was revised to apply the terms in the correct manners, which lead to a deeper understanding of awareness and training.

6.3.4. Expert Review Process: Round 4

In the final round of review which took place three months after round 3, the research project was presented at the annual ISSA security conference in Johannesburg. A discussion of the main concepts and contributions of the research project was provided. All the experts and those involved in the discussion were in agreement with the study’s proposed behavioural intention model and information security awareness process and thus final consensus was obtained.

Together, the analysis of the literature study and the expert reviews that were collected and the changes that were made as a result of it, supplied the necessary data to develop a refined behavioural intention model and information security awareness process. This was designed to essentially help reduce the risks the employees pose to firms and help move towards a positive information security culture.

6.4. Relevance and Validity of the Action Research at CEF

The action research at CEF tested the relevance, feasibility and applicability of the information security awareness process and behavioural intention model. The goals were to refine and test their real life applicability. The information security process and the behavioural intention model is meant to assist in moulding employee behaviour by providing relevant adequate training hence is was important to first explore how

employees security behaviour could be improved. Whenever a solution to a problem is thought to be found it is necessary to verify, refine and test it.

Action research is known to be a suitable research strategy for initial testing and possible adjustment of an approach. Furthermore, action research aims to help the participants to investigate reality in order to change it. This was also the goal of this study: to study and achieve organization-wide changes to prevailing practices. For these reasons, action research was selected as the research strategy.

Action research intervention at CEF was set in a multivariate social situation. It was conducted with all the employees of the company involving varying relationships between the participants. In addition, the research involved complex business relationships between CEF and its customers and partners. These relationships created a need for an increased security. This was necessary for protecting CEF's innovations as well as customers' and partners' sensitive information. The prevailing situation inside the firm was also complex as many of the employees considered the management passive in promoting information security issues, which made the prevailing situation at CEF challenging from the viewpoint of the intervention.

6.5. Evaluation

Research evaluation is a necessary step in order to ensure the credibility and integrity of the research project. Oates (2006) provides a set of equivalent criteria for positivist and interpretivist research. These are shown in Table 6.6.

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

Table 6.6: Quality in Positivist and Interpretivist Research (Oates, 2006)

As this is an interpretivist study, the interpretivist criteria apply to this research as follows:

1. Trustworthiness: With respect to the Delphi technique employed to evaluate the artifacts produced, the trustworthiness of the experts used to refine the research model was evaluated. The experts used in this process are respected in their respective field. Experts were selected from information security management research. Thus, the recommendations made by these experts can be considered trustworthy.

2. Confirmability: This criterion has been met through the use of multiple data collection techniques culminating in the action research and expert review in order to confirm the outcome of the research. The action research findings confirmed the theoretical findings. This led to the development of a refined information security process and behavioural intention model which was then also confirmed through expert reviews.

3. Dependability: Dependability is established through the use of literature from recognised authors and the contribution from experts in the field of study in the form of the expert review. The use of established theories and models that have been tested in numerous research projects add to the dependability of this project. The theories and models used in this study include: Theory of Reasoned Action, the Protection Motivation Theory and the Behaviourism Theory.

4. Credibility: Credibility has been achieved through the use of multiple data collection techniques and the use of expert review (as described with regards to confirmability).

5. Transferability: Transferability has been achieved as the research model can be applied to other inter-organisational settings with similar characteristics to CEF.

Through the application of these five criteria, the research project can therefore be considered credible. In addition, Hevner, et al. (2004) provide five options for evaluating interpretivistic research. These evaluation methods are depicted in Table 6.7.

1. Observational	Case Study: Study artifact in depth in business environment Field Study: Monitor use of artifact in multiple projects
2. Analytical	Static Analysis: Examine structure of artifact for static qualities (e.g., complexity) Architecture Analysis: Study fit of artifact into technical IS architecture Optimization: Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact behaviour Dynamic Analysis: Study artifact in use for dynamic qualities (e.g., performance)
3. Experimental	Controlled Experiment: Study artifact in controlled environment for qualities (e.g., usability) Simulation. Execute artifact with artificial data
4. Testing	Functional (Black Box) Testing: Execute artifact interfaces to discover failures and identify defects Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artifact implementation
5. Descriptive	Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility Scenarios: Construct detailed scenarios around the artifact to demonstrate its utility

Table 6.7: Design Evaluation Methods (Hevner, et al., 2004)

This research project made use of the following evaluation techniques:

1. Observational: Action research allowed the researcher to be able to monitor and observe the general security trends at a close range and this informed the refinement of the research artifact.

2. Analytical: This research project made use of expert reviews to analyse the structure, fit and performance of the artifact. The outcomes of these expert reviews were incorporated into the final research artifact.
3. Experimental: The artifacts where tested as an experiment at CEF and seemed to have been a successful experiment.
4. Testing: Testing was conducted at CEF and the results of the tests have been discussed in the prior sections.
5. Descriptive: The literature review and the under lining theories help to build a strong argument of the applicability of the research artifacts.

Through the use of these evaluation methods, the research project is considered to have met the requirements of action research and thus is a valid action research project.

6.6. Recommendations

6.6.1. Recommendations to the Firm

Given the initial lack of information security awareness, the recommendations provided here are meant to guide this or any other similar firms on how to effectively run and manage information security awareness programs.

- There is need to document and store lessons learnt from problem situations in order to apply these to future situations and avert further costly delays on the production line.
- Additionally, the firm can benefit from the creation of a “yellow pages” application which can direct employees to the necessary expert when a problem occurs, e.g. a computer has a virus, or when security breach is suspected. This would reduce the time spent searching for the relevant expert to aid in the problem.
- Furthermore, in order to keep at par with the ever-changing information security technologies and risks posed by the employees, it is advisable to run the process every 12 months.
- Employees need to be made aware of the importance of their own effort to the realisation of the overall organisational goals.

6.6.2. Recommendations for Further Research

This research study explored the risks exposed by the uninformed naïve employee. However the risks exposed by the malicious insider as well as the outsider still require exploration. This research study could have embarked on these as well but could potentially have uncovered countless other areas of interest in this context which would have made this research difficult to manage. This, however, was left for further research possibilities.

Future research should address the shortcomings pointed out by the literature review. Consequently, studies that develop theory-based cognitive and behavioural information security awareness approaches are called for. In addition, the practical efficiency of such approaches should be empirically explored. This holds for all cognitive approaches. This dissertation presented research agendas for information security awareness training and campaigns basing on the Theory of Reasoned Action the Protection Motivation Theory and the Behaviourism Theory. In the behavioural approaches, rewards and punishments have not been explored in the context of information security and hence studies that empirically explore their practical efficiency are welcome.

Lastly, the author recognises that although e-learning is not a novel idea, it is a relatively new aspect in the field of information security which has a great potential of resulting in e-security awareness initiatives. This study area will become more apparent as e-learning within information security expands.

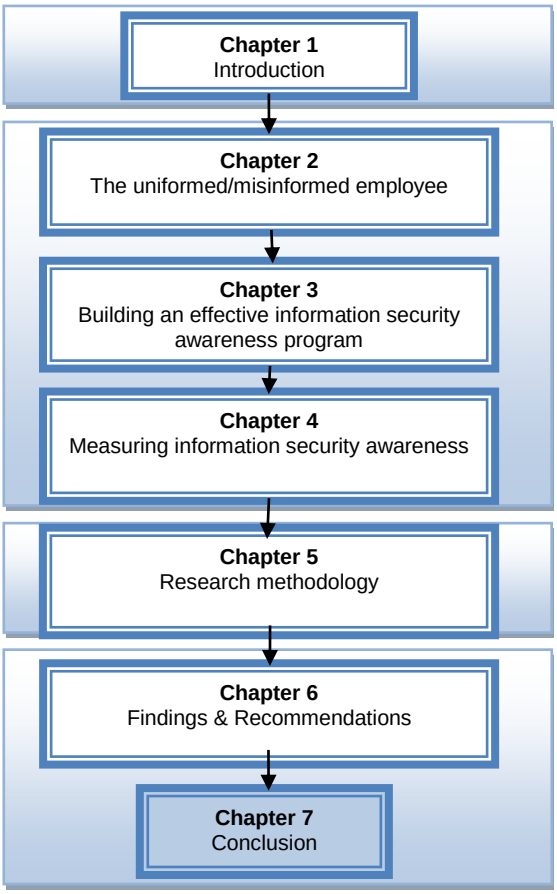
6.7. Conclusion

This chapter provides a discussion of the findings of this research study as they relate to the research problems presented in Chapter 1. An Information Security awareness and process is proposed to assist firms in implementing information security components in such a manner that they would positively direct employee behaviour towards the protection of information assets. As such, a model to enhance information security culture that promotes acceptable information security behaviour was designed, validated through expert review and refined and tested through action research.

The findings from the document survey, participant observation online surveys and the informal interviews were presented. The findings of the document survey proved to be of little use to this research study. It did however become apparent that insufficient emphasis is placed at CEF in this regards. The participant observation revealed password sharing and antivirus disabling provided majority of the findings for participant observation for this research study. This highlighted the apparent disregard for the value of CEF, and the need for this firm to take advantage of the opportunities available to them to improve on current operations. 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 participate in to get an information security awareness certificate valid for one year as discussed in the preceding chapter. The informal interviews were a rich source of information to identify the state of the information security at CEF before any intervention. A representative of every department in the firm was chosen randomly as part of the participant list.

The research findings showed that information security awareness levels are greatly influenced by behavioural intentions. The study has also been able to validate e-learning as an effective method of learning just as the traditional classroom style of learning. In conclusion the model and process presented in this dissertation is credible as seen by the results of the action research conducted. This has encouraged positive change in behaviour as observed during the iterations. Future research could focus on models and theories that assist in improving employee attitude as the behavioural intention model has proven to only impact on knowledge and behaviour and not the employees' attitude. The next Chapter summarises and concludes the study.

CHAPTER 7 - CONCLUSION



Chapter 7:

7.1. Introduction

The previous chapter discussed the findings and recommendations of the study. This chapter will provide a summative conclusion to the study and begins by providing a brief description of the research objectives of the study and the chapters that they have been met and the relevant supporting literature and previous studies. Table 7.1 below summarises the research objectives of the study and the chapters in which they have been discussed.

Research objective	Chapters	Research approaches
What are the attributes that affect employees' behaviour towards information security?	II, III	Literature review, conceptual analysis

What are the best ways to educate employees in order to raise their information security awareness levels?	III, V	Conceptual analysis, constructive research, and theory testing with action research
How should information security levels be measured so as to assess the need for training, or assess the effectiveness of an awareness or training session?	IV, V	Literature review, conceptual analysis, and theory testing with action research

Table 7.1: Research Objectives and Chapters They Are Addressed

The remainder of this chapter will be structured as follows, firstly brief conclusive discussions for every chapter, followed by a brief future research discussion. Finally strengths and limitations of the study are discussed.

7.2. Literature

It is well documented in literature that information security precautions being carried out mainly focus on reducing the risk of outsiders trying to access a firm's information assets. Literature further reveals that although the outsiders pose risk, the insiders pose almost the same risk but little or no precautions are being taken. It is however much more difficult to detect bad security behaviours of the employees as technical guards usually focus on detecting outsider intrusion.

Literature has also revealed significant information security problems that affect employee behaviour towards complying with information security policies. This then exposes them and the firm to numerous vulnerabilities such as viruses, social engineering scams, and improper usage of the corporate information asset. These vulnerabilities consist of a wide range of weaknesses specifically targeted by outsiders trying to get access though unsuspecting insiders. A detailed study of literature was conducted to identify the vulnerabilities that exist. Literature has revealed that information security awareness may go a long way in probing the vulnerabilities. The Protection Motivation Theory, Theory of Reasoned Action and the Behaviourism Theory as identified by literature assist in explaining how employees intend to behave and the elements that influence their behavioural intentions.

7.3. Research Questions

The research question that this study investigates is: *How can Engineering SMEs in emerging economies cultivate positive employee behaviour towards information security?* The main objective of this research project is to design, refine and validate an information awareness process that can be followed by any Engineering SME firm when planning and implementing an information security awareness program. To answer the main research question, three sub-research questions were identified:

1. What are the attributes that affect employees' behaviour towards information security?

This sub-question was addressed in Chapter 4 and 5 and the theories that explain employee behavioural intentions were identified and these are the Theory of Reasoned Action, the Protection Motivation Theory and the Behaviourism Theory. The theoretical basis assisted in formulating the proposed behavioural intention model. The theories assisted in establishing an accurate and logical argument to support the proposal of this model.

2. What are the best ways to educate employees in order to raise their information security awareness levels?

This sub-question was addressed in Chapter 3 during literature review and the current information security awareness techniques used were examined and the communication modes were discussed. In these chapters it was highlighted that current techniques used are not effective enough as employees still exhibit signs and symptoms of ignorance. Additionally, this sub-question was discussed in Chapter 5. In this chapter it explained how the proposed information security awareness process will educate employees in the art of safe information security practices.

3. How should information security levels be measured so as to assess the need for training, or assess the levels of awareness or effectiveness of a training session?

Chapter 4 and 5 addresses the third and last research sub-question. Chapter 4 examined information security measuring frameworks and methodologies. These models highlighted different aspects of measurement and explained ways in which measurements should be conducted within the context of information security awareness. Chapter 5 adapts one of the information security awareness concept discussed in Chapter 4. The study adapted Kruger and Kearney's (2005) information security measuring model.

7.4. Theoretical Frameworks

Three theoretical frameworks were used to explain the behaviour of employees towards information security. These are the Theory of Reasoned Action (TRA), the Protection Motivation Theory (PMT) and the Behaviourism Theory (BT). According to Anderson and Agarwal's (2010) 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 (Hogg & Abrahams, 1988).

7.4.1. Theory of Reasoned Action

TRA framework specifically evaluates the relative importance of two incentive components i.e. attitude and subjective norm. It advocates that an employee's Behavioural Intention (BI) depends on his/her Attitude (A) about the behaviour and Subjective Norms (SN) i.e. (BI = A + SN).

7.4.2. Protection Motivation Theory

Information security awareness and training instils knowledge in 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. It is composed of the following two items, i.e. perceived vulnerability perceived severity

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. Coping appraisals are made up of three sub constituents i.e. self-efficacy, response efficacy and response cost

Previous research that used PMT found it useful in predicting behaviours related to an individual's computer security behaviour both at home and in the work situation as well as Information Security Policy (ISP) compliance.

7.4.3. Behaviourism Theory

According to Skinner (1965) the Behaviourism Theory loosely encompasses the work of other behavioural 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: Firstly, 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 i.e. classical conditioning and operant conditioning.

7.5. Research Methodology

In this section the research methodology is summarised. The research follows a qualitative approach, and performed expert reviews abiding by the review process. This provided the necessary evaluation and refinement of the proposed solution. Additionally, the various paradigms considered in research were presented, and it was determined that the study mostly applies to an interpretivistic view. Therefore, this research was conducted in the form of an action research. Action research allows for simultaneous practical problem solving and refinement of scientific knowledge. This goal extends into two important process characteristics: First, there are highly interpretive assumptions

being made about observation; second, the researcher intervenes in the problem setting. This study presents a detailed example of an action research process of design, along with the process that should be followed when designing an information awareness program. This research project proposes a process based on both primary and secondary data, and is further refined by the expert reviews which were performed. Justification is made as to why action research was chosen as the most appropriate approach to be adapted by this research project, and the reasons for using expert reviews were presented.

Expert reviews formed part of the primary data collection and assisted with analysis and giving feedback that was useful for re-evaluation. The reason that expert reviews were selected as the primary source of data collection for this study was because experts in the information security awareness domain have 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 developing 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 can be obtained. The expert reviewers were approached with flexibility, thus allowing the experts the freedom to respond according to their unique opinions and judgements.

7.6. Results and Findings

A 78% awareness level was achieved after the third iteration of the information security awareness process of the action research. This was satisfactory enough to temporarily pause further iterations. However, it is advisable to run the process at least once a year as the skills and knowledge of the employees may become outdated.

This study revealed 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 firms' stance (subjective norm) on information security, threat appraisal, coping appraisal and try 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 the employees' security knowledge levels were very low, they had a positive attitude towards securing the firm's information asset; however, they did not have the skills and knowledge to behave in a secure manner. This also helps to confirm that indeed the risk that employees expose the firm to is genuinely 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 is most likely because employees have a certain attitude towards the firm and this attitude cannot be altered by information security awareness alone.

7.7. Evaluation and Validation of the Research

After refinement of the research project in the expert review process, and with a more thorough investigation during the action research, refined process and model was developed which sought to provide firms the steps to follow when running information security awareness initiatives.

Evaluation and validation of the study is reflected in detail within the research methodology of the approach used. Twelve experts in the online trust and security field were presented with the findings of the research and requested to comment on the correctness and applicability to the research problem, to further refine the artifact being developed. Expert review is a popular method that is widely used and accepted to gather data from respondents. The technique is designed as a collective communication process aimed at a group of individuals with the objective to obtain a wide variety of expert opinions on specific real-world problems. The expert review conducted in the study consisted of four rounds of review, analysis and feedback.

The first round was validated by three experts who provided an extensive critical review of the information security process, concepts and they questioned if the proposed model would change behaviours of malicious insiders. A second round of the validation process occurred, which resulted in less extensive, but highly valuable feedback from a different set of three reviewers. In the third round of validation, the largest response was seen as five experts were consulted. The opinions and comments obtained in this round were found to be extremely influential in constructive criticism, successfully improving the proposed process and model on all levels. Finally, the fourth round resulted in strong agreement and consensus from the particular experts who were provided with an opportunity to respond. Throughout the review process, all responses and comments made were taken into account and accordingly 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 that occurred, thereby making the research study of an increasingly credible standard. Therefore, the way in which the review process was conducted was deemed to be credible, leading to a perception of a trustworthy study.

Although, the dependability of the responses received from the experts is difficult to measure. It is heavily dependent on the experts who were involved in the review process, their position and expertise, the situation, expectation and own perception on the subject. Therefore, the expert review process was conducted in a non-leading manner using defined research data presented for analysis, with the aim of keeping the process as open as possible.

The secondary data collected included literature from 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 objectives. This was most important, as it identifies the body of knowledge of which the study will be based on and expand upon. By combining these two data

collection methods, and using them as inputs into a design science approach, innovative artifacts were able to be developed.

De Vos et al. (2005) note that dependability and trustworthiness are important in document study. To ensure and increase the dependability of the literature used in this study, only well-known researchers, authors and institutions have been used in the construction of the theoretical framework. In general, credibility and dependability of this study have been achieved.

7.8.Future Research

The study was positioned in the context of the security behaviours of the naïve/ignorant employee. It focused specifically on the methods of raising information security awareness levels of employees. This research study explored the risks exposed by the uninformed naïve employee to Engineering SMEs' information assets. However, the risks exposed by the malicious insider as well as the outsider still require exploration. Future research could include researching methods of combating risks posed by the malicious insider and outsider. The objective of this future research could be to eliminate any redundancies that may have been caused by not including them in the proposed process and model, or to cover any unforeseen gaps that may develop in the future.

7.9. Strengths and Limitations of the Study

The researcher hopes that this study has made a contribution to information security awareness research. In particular with regard to moulding behavioural intentions of employees in Engineering SMEs to address the problems highlighted in current literature. It is hoped that this research study sparks 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 conference paper presented at the Information Security South Africa (ISSA) conference in 2012. I was awarded the best paper at the conference. Another paper has been submitted for journal publication and is currently under review.

The researcher acknowledges the lack of extensive critical review of literature relating to measuring employee awareness levels. Current literature relating to this context reveals limited methods of measuring awareness and thus did not provide sufficient basis for a critical review.

With regards to the findings of this study, CEF restricted the findings of this research study to Engineering SMEs. The researcher realises that the firm selected for this study was not representative of all SMEs. Ideally this study would have had multiple interactions within different industries. Due to time and financial constraints it was not feasible. It was however still significant to use it as an example to discover how information security awareness initiatives are handled by SMEs operating in South Africa to test the process and model presented in this study.

7.10. Summary

The value of this study can be determined by the impact it had on the CEF's information security awareness program implementation, it increased levels of awareness of employees reducing the risk of costly naïve mistakes. This in turn improved the success of the firm as it reduced downtime caused by virus attacks and other information security incidences. Overall, information security awareness is crucial for Engineering SMEs because usually they will not have enough resources for recovery from incidences.

This dissertation consisted of three research steps. The first step of this dissertation was to reviewing and evaluating the state of the existing literature. The second step was to design and refine an information security awareness process that can be followed by Engineering SMEs in emerging economies. The final step was to practically test the process and evaluate its practicality.

LIST OF REFERENCES

Anderson,C.L., and Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*. Vol 34(1), pp. 613-43.

Ajzen,I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*. Vol 50(2), pp. 179-211.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes*, Vol 50(2), pp. 248-87.

Baskerville, R. L. (1999). Investigating information systems with action research. *Communications of the AIS*, Vol *2*(3es), pp. 4.

BERR. “Information Security Breaches Survey” – Technical Report. Department for Business Enterprise and Regulatory Reform. April 2008. URN 08/788.

Boeckeler, M. C. (2004). Overview of Security Issues Facing Computer Users. *SANS Institute, InfoSec Reading Room*.

Brodie, C. (2008). The Importance of Security Awareness Training. *SANS Institute, InfoSec Reading Room*.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, Vol 34(3), pp. 523-48.

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 http://www.cert.org/archive/pdf/ecrimesummary10.pdf.

CSO magazine, U.S. Secret Service, CERT, Deloitte. (2010). *2010 Cyber Security Watch Survey*.

Chipperfield, C., and Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security*, Vol 2010(3), 13-19.

Collis, J., and Hussey, R. (2009). *Quantitative Methods for Business and Management (3rd Edition).* 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*, Vol 14(4), 186-196.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behaviour.* Vol 28(5), pp. 1849–1858.

Danchev, D. (2003). *Building and Implementing a Successful Information Scurity Policy.* Retrieved May 13, 2009 from www.windowsecurity.com.

Da Veiga, A., and Eloff. J.H.P. (2010). A Framework and assessment instrument for Information Security Culture, *Computers & Security*, Vol 29(2), pp. 196-207.

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 Publishers*.

Du Plessis, L., and Von Solms, R. (2002). Information Security Awareness: Baseline Education and Certification. *INFORMATION TECHNOLOGY ON THE MOVE*, pp. 101.

Elden, M., and Chisholm R.F. (1993). Emerging Varieties of Action Research: Introduction to the Special Issue, *Human Relations.* Vol 46(2), pp. 121-142.

Eminağaoğlu, M., Uçar, E., and Eren, Ş. (2009). The positive outcomes of information security awareness training in companies–A case study. *Information Security Technical Report*, Vol *14*(4), 223-229.

Etsebeth, V. (2006). Information Security Policies - The Legal Risk of Uninformed Personnel. *ISSA.* Sandton , Johannesburg.

Fishbein, M., and Ajzen, I. (1975). *Belief, attitude, intention, and behavior: 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*. Vol 2006(9), pp. 8-12.

Furnell, S., and Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security*, Vol *2012*(3), 12-15.

Furnell, S., and Thompson, K. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security *Computer Fraud & Security*. Vol 2009(2), pp. 5-10.

Flowerday, Sand Von Solms, R. (2005). Real-time information integrity = system integrity + data integrity + continuous assurances. *Computers & Security* 24(8), 604-613.

Hale, J. L., Householder, B. J., and Greene, K. L. (2003). 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.

Herath, T., and Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, *Decision Support System*, Vol 47(2), pp. 154 – 165.

Hinson, G. (2006). “Seven myths about information security metrics,” originally published in ISSA Journal, Available at: http://www.noticebored.com/html/metrics.html (Accesed Feb. 2010)

Hofstee, E. (2006). Literature Review. In *Constructing a good Dissertation*. Johannesburg: EPE.

Hogg, M.A., and Abrahams, D. (1988). *Social identifications: A social psychology of intergroup relations and group processes*. Routledge, London and New York.

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

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security.* Vol 31(1), pp. 83-85.

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).

ISO 27002, (2005). Code of Practice for Information Security Management as a base for Certification.

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*. Vol 59(2), pp 255−259.

Johnson, E. (2006). Security Awareness: Switch to a better program. *Network Security*. Vol 2006(1), pp 15-18.

Johnstone, M. (2001). Seurity Awareness Training and Privacy. *SANS Institute, Infosec Reading Room* .

Kabay, M. E. (2004). *Whats important for Information Security: A Managers Guide*. Norwich University.

Kabay, M.E. (2005). Improving Information Assurance Education Key to Improving Secure(ity) Management. *Journal of Network and Systems Management*. Vol 13(3), pp 247-251.

Kruger, H. A., and 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*, Vol *25*(4), pp. 289-296.

Krutz, R. L., and Rusell, D. V. (2001). *The CISSP Prep Guide.* New York: John Willey & Sons.

Lee, Y., and Larsen, K.R. (2009). 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.

Milne, S., Sheeran, P., and Orbell, S. (2000). Prediction and intervention in health-related behavior: a meta-analytic of protection motivation theory. *Journal of Applied Social Psychology*, Vol 30(1), pp 106-43.

Miller, K. (2005). *Communications theories: perspectives, processes, and contexts.* New York: McGraw-Hill.

Nosworthy, J.D. (2000). Implementing Information Security In The 21st Century – Do You Have the Balancing Factors? *Computers & Security,* Vol 19(2), pp. 337 – 347.

Pahnila, S., Siponen, M., and Mahomood, A. (2007). Employees' behavior towards IS security policy compliance, *Proceedings of the 40th Hawaii International Conference on System Sciences*, January, pp. 3-6, Los Alamitos, CA.

Pechmann, C., Zhao, G., Goldberg, M., and 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.* Vol 6, pp. 1-18.

eltier, T. R. (2005). Implementing an information security awareness program. *EDPACS*, Vol *33*(1), pp. 1-18.

Pfleeger, S. L., and Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security,* Vol 31(3), pp. 597-611.

Power, R. (2002). CSI/FBI Computer Crime and Security. *Computer Security Journal,* Vol 17(1) , pp. 7-30.

Reynold, G.S. (1975). *A primer of operant conditioning*. (Rev ed). Glenview, IL: Scott, Foresman.

Richardson, R. (2008). CSI Computer Crime and Security Survey. CSI, 2008. Available from: http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf (Accessed 14 December 2009).

Ricer,R.E.,Filak, A.T., and 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*. Vol 17(2), pp. 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*, Vol *52*(3), pp. 596.

Rogers, R. (1983). 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.

Russell, C. (2002). Security Awareness - Implementing an Effective Strategy. *SANS Institute, InfoSec Reading Room*.

Sarkar, R.K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures, *Information Security Technical Report.* Vol 15(15), pp. 112-133.

Schaffers, H., Guzman, G., and Merz, C. (2008). An Action Reaserch Approach to Rural Living Labs Innovation. 2*Universidad Carlos III de Madrid.*

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.

Skinner, B.F. (1965). *Science and human behavior*. Columbus: Free Press.

Smart, K.L., and Cappel, J.J. (2006). Students' perceptions of online learning: A comparative study. *Journal of Information Technology Education*. Vol 5, pp. 201−202.

Sookdawoor, O. (2005). An Investigation of Information Security Policies and Practices in Mauritius. UNISA, Johannesburg.

Staats, A.W., and Staats, C.K. (1958). Attitudes established by classical conditioning. *The Journal of Abnormal and Social Psychology* Vol 57(1), pp 37-58.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, Vol *24*(2), pp. 124-133.

Stephanou, A. T., and Dagada, R. (2006). The Impact of Information Security Awareness Training on Information Security Behaviour: The case Study for further Research. *University of Witwatersrand,* Johannesburg.

Talaei-Khoei, A., Solvoll, T., Ray, P., & Parameshwaran, N. (2012). Maintaining awareness using policies; Enabling agents to identify relevance of information. *Journal of Computer and System Sciences*, Vol *78*(1), pp. 370-391.

Van Niekerk, J., and Von Solms, R. (2004). Organisational Learning Models for Information Security*. Peer reviewed Proceedings of the ISSA 2004* enabling tomorrow conference 30 June – 2 July 2004, Gallagher Estate, Midrand.

Van Niekerk, J, and Von Solms, R. (2010). Information Security Culture: a management perspective. *Computers & Security*. Vol 29, pp. 476-86.

Von Solms, B., and Von Solms, R. (2004). The 10 deadly sins of information security management. *ELSEVIER - Computers & Security, Vol 23* , pp. 371-376.

Voss, B. D. (2001). The Ultimate Defense of Depth: Security Awareness in Your Company. *SANS Institute, InfoSec Reading Room*.

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*, Vol 13(4), pp. 207-215.

Williams, P. A. (2009). What does security culture look like for small organizations?. *Proceedings of the 7th Australian Information Security Management Conference (Perth, Australia, 2009), pp. 48-54.*

Wilson, M. and Hash, J. (2003). Building an Infomation Technology Security Awareness and Training Program. *National Institute of Standards and Technology*.

Willson, R. and Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through situational crime prevention. *Communications of the ACM*. Vol 52. NY, USA.

Wood, B. (2000). An insider threat model for adversary simulation. *SRI International, Research on Mitigating the Insider Threat to Information Systems*, Vol *2*, pp. 1-3.

Woon,I.M.Y., Tan,G.W., and Low, R.T. (2005). A protection motivation theory approach to home wireless security. In: D. Avison, D.Galletta and J.I. DeGross, editors. *Proceedings of the 26th International Conference on Information Systems*, In Las Vegas, December 11-14, pp. 367-380; USA.

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 Behavior*, Vol *24*(6), pp. 2799-2816.

LIST OF ABBREVIATIONS

A	Attitude
BI	Behavioural Intention
BT	Behaviourism Theory
CD-ROM	Compact Disc Read Only Memory
DOS	Denial Of Service
DVD	Digital Video Disc
GIS	Geographical Information Systems
ICT	Information and Communication Technologies
IS	Information Systems
ISP	Information Security Policy
ISSA	Information Security South Africa
PDF	Portable Document Format
PMT	Protection Motivation Theory
SME	Small to Medium Enterprises
SN	Subjective Norm
TRA	Theory of Reasoned Action

APPENDICES

Appendix A

For Institutional Users:
Institutional Sign In
Athens/Shibboleth

Browse Conference Publications > Information Security for Sout ...

The enemy within: A behavioural intention model and an information security awareness process

This paper appears in:
Information Security for South Africa (ISSA), 2012
Date of Conference: 15-17 Aug. 2012
Author(s): Gundu, T.
Dept. Inf. Syst., Univ. of Fort Hare, East London, South Africa
Flowerday, S.V.
Page(s): 1 - 8
Product Type: Conference Publications

Available Formats	Non-Member Price	Member Price
PDF	US$31.00	US$13.00

Learn how you can qualify for the best price for this item!

ABSTRACT

Most employees in small and medium enterprise (SME) engineering firms now have access to their own personal workstations which have become part of their daily functions. This has led to an increased need for information security management to safeguard against loss/alteration or theft of the firm's important information. SMEs tend to be 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 controlling them do not have adequate information security knowledge. This tends to expose the firm to costly mistakes that can be made by naïve/uninformed employees. This paper presents an information security awareness process that seeks to cultivate positive security behaviours using the behavioural intentions models i.e. the Theory of Reasoned Action and the Protection Motivation Theory. The process presented has been tested at an SME engineering firm, and findings are also presented and discussed in this paper.

INDEX TERMS

- **IEEE Terms**
  Appraisal , Electronic learning , Guidelines , Information security , Training
- **INSPEC**
  - **Controlled Indexing**
    authorisation , computer viruses , small-to-medium enterprises
  - **Non Controlled Indexing**
    SME , antivirus software , behavioural intention model , behavioural intentions models , firewalls , information security awareness process , information security management , personal workstations , protection motivation theory , security incidents , small and medium enterprise
- **Author Keywords**
  Information Security Awareness , Security Behaviour

Additional Details

Topic(s) : Communication, Networking & Broadcasting ; Components, Circuits, Devices & Systems ; Computing & Processing (Hardware/Software)
Conference Location : Johannesburg, Gauteng
Print ISBN: 978-1-4673-2160-0
INSPEC Accession Number: 13038614
Digital Object Identifier : 10.1109/ISSA.2012.6320437
Date of Current Version : 04 October 2012
Issue Date : 15-17 Aug. 2012

Appendix B

This CD-ROM contains copies of the information security awareness campaigns/training and the assessment tests. Please note that the company logos and slogans have been removed for anonymity reasons.