THE IMPACT OF INFORMATION SECURITY AWARENESS TRAINING ON INFORMATION SECURITY BEHAVIOUR

ANTHONY STEPHANOU

A RESEARCH REPORT SUBMITTED TO THE FACULTY OF COMMERCE, LAW AND MANAGEMENT, UNIVERSITY OF THE WITWATERSRAND, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF COMMERCE

Johannesburg, 2008

ABSTRACT

Information Security awareness initiatives are seen as critical to any information security programme. But, how do we determine the effectiveness of these awareness initiatives? We could get our employees to write a test after the awareness to determine how well they understand the policies, but this does not show how they affect the employee's on the job behaviour. Does awareness training have a direct influence on the security behaviour of individuals, and what is the direct benefit of awareness training? This research report aims to answer the question: To what extent does information security awareness training influence information security behaviour?

Technologies meant to provide security ultimately depend on the effective implementation and operation of these technologies by people. Thus awareness of policies is needed by all individuals in an organisation to ensure that policies are well understood and not misinterpreted. Some researchers have maintained that educating users is futile mainly because it is believed that it is difficult to teach users complex security issues and, secondly, because if security is seen as secondary by the user they will not pay enough attention to it.

This research found that, firstly, there is a shortage of in-depth information security awareness research and that behavioural concepts are not properly taken into account for security awareness programmes. There is a shortage of theoretical models explaining how awareness training affects behaviour. Secondly, this research tested a proposed model empirically using system-generated data as indicators of behaviour in a pretest-posttest experimental design. It was found that security awareness training was effective in terms of end-users retaining security knowledge. However, there was no evidence to suggest that security awareness by itself is sufficient to ensure compliant behaviour by end-users. Security awareness training is a necessary, integral component that could influence compliant behaviour, but is not adequate to do so fully. Practitioners must insist that their security awareness programmes are measured in terms of effectiveness and focus on behavioural aspects to complement traditional security awareness initiatives.

DECLARATION

I, Anthony Stephanou, declare that this research report is my own work except as indicated in the references and acknowledgements. This report is submitted in partial fulfilment of the requirements for the degree of Master of Commerce in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or in any other university.

Anthony Stephanou

Signed at Johannesburg

On the 18th day of December 2008

ACKNOWLEDGEMENTS

I would like to thank the following people without whom this research would not have been possible:

- Ashney Chetty, for her love, patience and generosity;
- my family for their words of support;
- my supervisors: Jens Mende and Rabelani Dagada;
- Professor Jason Cohen for his advice;
- Professor Jeffrey M Stanton for his inspiration;
- Charl van der Walt for his data collection assistance and,
- finally to all the participants for their support and cooperation.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1 : INTRODUCTION

Users are much more likely to support and comply with policies if they clearly understand the purpose for the policies and their responsibilities in regard to the policies.

Information Security Manager for an American state agency (GAO, 1998:49)

We live in an age where information is becoming more and more valuable (Trompeter & Eloff, 2001:384) and the success of an organisation will to a large extent depend on the availability of its information (Finne, 2000:234). People expect 24/7 access to public and private networks and expectations of users are growing. In addition, there are increased dependencies on third parties owing to collaborative efforts, continuous monitoring for support purposes or outsourcing development. Organisations are coming to terms with their growing dependence on information and the related communication and information technology (IT) components that house and process this information. They are learning how to harness these for continued success.

With this increased reliance on IT, organisations, particularly financial institutions, are facing escalating information security threats and the associated potential impact is also escalating as their dependence on IT grows. This has been highlighted by ongoing news reports, independent security surveys and other similar reports (Deloitte 2006 Security Survey, 2006:13, OECD, 2002:7). The reasons for this increase in security threats is mainly due to complexity in systems (Schneier, 2000,6), convergence of technologies and the interconnected nature of systems (OECD, 2002:7).

IT systems are dependent on people. Schneier (2003:10) maintains that information security is more about behaviour than anything else, that is, getting people to behave in a certain way. Security wants to prevent people's intentional actions and the associated adverse consequences. Despite the hype from vendors about the need for security products many critical security activities have not and cannot be automated. Technologies meant to provide security ultimately depend on the effective implementation and operation of these technologies by people. This means that organisations are dependent on people to achieve a secure environment. Since humans are seen as the "weakest link" in the information security chain (Schneier, 2000; Stanton, Stam, Guzman &

Caldera, 2003:1; Katsikas, 2000:130; van Niekerk & von Solms, 2004:2; von Solms, 2000:618), there is a clear requirement to ensure users are trained correctly in terms of information security policies. The goal is to ensure that users firstly use the necessary policies and thereafter to ensure that they are not misused or misinterpreted thereby ensuring the effectiveness of policies (Siponen, 2000a:31). Security awareness efforts are seen as the "first line of defence" (OECD, 2002:10).

A very real and increasing threat is that of insiders. Insiders are company staff, authorised individuals, who have privileged access to IT systems, understand the internal processes of the organisation and may have some level of technical expertise. All these factors together pose a serious threat to the organisation. Insider threats do not only include malicious actions but even neutral and accidental errors/threats to the organisation. Since the internal threat is a result of incorrect security behaviour (Leach, 2003:685) it follows that security awareness initiatives to encourage and demonstrate appropriate behaviour is a good idea. The OECD guidelines on securing information systems (OECD, 2002:8) agree, calling for a "culture of information security", that is, introducing a new way of thinking and behaving when working with information systems.

In January 2001, after completing a study the Department of Transport in the United States recommended that all agencies need to focus on employee awareness in order to protect the nation's critical infrastructure. This stemmed from a Presidential Decision Directive 63, issued by President Clinton in May 1998, requiring agencies to protect the information systems that support the nation's critical infrastructure (FCW, 2001).

OECD guidelines also call for greater public awareness and understanding of security issues by those who develop, own, manage, service and use information systems – whether at a policy or an operational level (OECD, 2002:7).

Thus security awareness is seen as essential to any organisation concerned about information security (Nosworthy, 2000; von Solms, 2000; Siponen, 2001; Janczewski & Xinli, 2002; OECD, 2002; Straub & Welke, 1998; GAO, 2005); however, is it effective in mitigating threats to the organisation?

Reporting on the progress of implementing information security statutory requirements in federal agencies, the Government Accountability Office (GAO) of the United States Congress testified to the house committee in April 2005. In summary, they reported that although there were improvements in addressing information security problems, significant security risks still existed. This is despite an improvement in awareness training initiatives by the agencies: 70% of all agencies trained 90% or more of their employees, as opposed to 54% of agencies in 2003 (GAO, 2005:16). This report raises a number of interesting questions:

- Did the increased awareness training make any difference to the security posture of the agencies, that is, was it effective? The report mentions that awareness was carried out as required but not whether it made a difference or not.
- The report did mention improvements in security but does not state whether this can be attributed to security awareness training.
- Did the training save money and prevent security incidents, that is, are the effects measurable? Perhaps the agencies would be better off spending relatively more money on other security initiatives if their effectiveness could be measured.

More research is required on the outcome and effectiveness of security awareness assignments (Schultz, 2004:1; Siponen, 2001:24). Information security research has always been skewed towards technical aspects of security (Siponen, 2001:24; Stanton et al. 2003:1; Trompeter & Eloff, 2001:384). However, it was soon recognised that focusing on technical issues alone is inadequate (von Solms, 2000: 615; Schneier, 2000:xi). Most of the awareness research concentrates on the importance of awareness initiatives (Nosworthy, 2000; von Solms, 2000; von Solms, 2001; Siponen, 2001; Janczewski & Xinli, 2002) and awareness techniques (Gaunt, 2000; van Niekerk & von Solms, 2004; Trompeter & Eloff, 2001; Katsikas, 2000; Johnston, Eloff & Labuschange, 2003; Thomson & von Solms, 1998) as opposed to research on the behavioural aspects of awareness initiatives (Siponen, 2001:26).

Many authors then argued that since “insiders” (personnel) pose the greatest security threat to an organisation, it follows that appropriate behaviour must be encouraged in order to enhance the organisation’s security position (Janczewski & Xinli, 2002:179; Leach, 2003:685; van Niekerk & von Solms, 2004:2; Stanton, Stam, Mastrangelo & Jolton, 2005:125).

Security management standards such as SABS ISO/IEC 17799 (SABS, 2000) and the Information Security Forum’s (ISF) The Standard of Good Practice (ISF, 2005) also support information security awareness initiatives. Unfortunately there is a shortage of in-depth research on information security awareness initiatives (Siponen, 2001:24) as will be demonstrated throughout this report.

Recent work in behavioural information security has shown: how employee job attitude relates to information security behaviours (Stanton et al., 2003); what categories of information security behaviours exist (Stanton et al., 2005); what influences information security behaviours (Leach, 2003); how attitudes and intentions are significant factors in explaining why some employees do not comply with information security policies (Pahnila, Siponen & Mahmood, 2007) and how a design theory for a security awareness programme was effective and was shown to achieve positive results, change user attitudes and, make users more conscious about their behaviour. More practical studies of this nature are called for (Puhakainen, 2006:106, 114, 139).

However, more research is required on the link between security awareness initiatives and the outcomes of such activities: in other words, the resultant behaviour of employees in organisations as a result of awareness activities. Schultz (2004:1) calls for further research on the benefits of information security awareness and training. Next, this chapter will describe why the research problem is important and how this report will help to address the research problem.

The purpose of this chapter is to demonstrate the following:

- A problem exists – security awareness training is considered critical, given the threats facing organisations. However, more research is required on the outcome of awareness training programmes.
- The problem is important – the impact of security breaches on organisations is potentially significant. The same is true if policies are not used, misused or misinterpreted.
- This research is necessary and will help to solve the problem – by measuring the effectiveness of awareness training on end-user behaviour lessons will be learned for more effective organisational awareness programmes.
- The research design is viable in order to help solve the problem.

1.1. THE IMPACT ON ORGANISATIONS IS POTENTIALLY SIGNIFICANT

The following is a sample of security incidents reported in the press over a two-month period in 2006:

- On 31 August, the UK Home Office admitted that its ID and passport services database had experienced five security breaches in the previous five years – four of them from so called "insiders" (SANS Institute (a), 2006).
- The Business Software Alliance (BSA) in the UK stated that

approximately 80% of software piracy cases that it gets involved in are due to “negligence and not malice”. It further urged the UK government to educate the public about software licences (SANS Institute, 2006a).

- An Indian call centre employee working in eastern India was arrested for allegedly using customer credit card information she obtained through her work to purchase items over the Internet (SANS Institute, 2006b).
- On 5 September, Microsoft Word 2000 users were warned of a flaw in the application that could allow external attackers to take remote control of a target workstation if the owner of the workstation opened a specific attachment. At the time of the report, Microsoft had not yet issued a patch for the vulnerability, and users were advised not to open un-trusted documents (SANS Institute (c), 2006).

These incidents are typical of what is reported in the press on a daily basis. In the first three quarters of 2003, 114,855 incidents and 2,982 vulnerabilities were reported to CERT®/CC. Obtaining consistently reliable statistics on the scale and impact of computer crimes and other security incidents is very difficult mainly because organisations want to avoid the associated negative publicity.

For example, in 2006 the Computer Security Institute (CSI) reported that even in an anonymous survey, only 50% of 616 US companies surveyed were willing to disclose the financial losses associated with a security breach. Of this group however, the survey did report the average annual loss of security breaches to be $167,713 (as a result of various reasons). Interestingly, there is a substantial increase in the importance of security awareness perceived by those surveyed. On average respondents felt that their organisations were under-investing in awareness at that time (Computer Security Institute, 2006).

The 2007 CSI Computer and Crime Security Survey shows a large increase in the average annual loss experienced by organisations compared to the previous year, jumping to $350,424. These organisations pointed at financial fraud as being the leading source of these losses (Computer Security Institute, 2007:2).

Another study from the University of Michigan quantified the cost of responding to 30 security-related incidents at $1million and 9,000 employee hours. An extreme example is the direct cost of the Code Red Worm outbreak in 2001, which was estimated at $1 billion (for recovering and protecting servers), and an additional $1.4 billion for indirect costs of the worm (such as lost productivity) (Madigan et al., 2004:47).

The impact of security breaches on organisations may not only lead to financial losses (which in themselves may be very difficult to quantify) but can also include nonfinancial and more subtle consequences. For a publicly listed organisation, incidents of data theft could lead to a range of consequences such as negative publicity, sanctions and tougher regulations imposed by regulators, potential litigation against the organisation, impact on market share, doubt in the organisation's systems and staff, and reduction in employee morale.

Internal abuses of security policies at the workplace (such as dealing in pirated software or pornography) may also have negative consequences to the organisation in terms of lost productivity. The 2007 CSI survey found that this type of abuse was the most prevalent security problem experienced by organisations surveyed (Computer Security Institute, 2007:2).

Thus, if an organisation does not manage security effectively, the impact to an organisation could be very significant. Security practitioners have known for years that information security is not just a technical issue anymore; it is a multidimensional discipline (von Solms, 2001b:504; Finne, 2000:235; von Solms & von Solms, 2001:308). Since the purpose of information security is to protect organisational assets from unauthorised use (von Solms & von Solms, 2000: 59) and the disciplines making up information security are related and interdependent, it follows that disregarding one of these leads to potentially significant risks to organisations (Von Solms, 2001b:507; von Solms & von Solms, 2001:308). One such discipline is security awareness efforts since end-user behaviour is seen as critical in the information security chain (Schneier, 2000; Stanton et al. 2003:1; Katsikas, 2000:130; van Niekerk & von Solms, 2004:2; von Solms, 2000:618) and, traditionally, relatively little attention has been paid to the importance of awareness training.

Awareness is important because attackers frequently take advantage of people's natural tendency to be helpful and forthcoming in order to get into a system (as opposed to attacking the system technically), also known as social engineering. For example, in 1994 a Frenchman called the FBI pretending to be an FBI representative and convinced the person on the other end of the line to help him connect to the FBI phone conferencing system. He then ran up a $250,000 phone bill over a number of months (Schneier, 2003:143).

The purpose of information security awareness is to inform a broad audience of information security policies using attention-getting and user-friendly techniques. The objective is to ultimately make them behave appropriately (Katsikas, 2000:130). This is intuitive since in any organisation employees cannot be expected to comply with policies unless they are aware of them and understand them.

Neumann (2003, 136), reporting to the US House of Representatives committee on computer-communications security in 2001 and later repeating his stance in 2003, maintains that information security is in fact getting worse relative to the risks. He concludes: "Even if an entire system has been subjected to extremely rigorous open evaluation and stringent operational controls, that may not be enough to ensure adequate behavior."

1.2. THIS RESEARCH WILL HELP TO SOLVE THE PROBLEM

Given the nature of risks they face, organisations could organise an awareness campaign and get their employees to write a test afterwards to determine how well they understand the policies. This, however, does not mean that the training improves employees' on-the-job behaviour. How do companies determine the benefits of awareness training? Do companies become more secure as a result of the end-users' becoming more security aware? If it can be shown that such training results in, say, less security incidents or more appropriate security behaviour, then obviously this could benefit organisations and industries.

More research is required on the link between security awareness initiatives and the outcomes of such activities: in other words, the resultant behaviour of employees in organisations as a result of awareness activities.

To this end, the following section will summarise the limitations of the existing research work on security awareness and thereby reinforce the necessity of this research. A more detailed discussion of the state of the existing security awareness landscape is presented in Chapter 2.

1.2.1. Limitations of existing research: the case for further research

Cognitive research approaches consider the individual to be an active processor of information and that their behaviour does not change unless the person has a meaningful understanding of information. In the context of security awareness research these approaches aim to change behaviour through persuasion using awareness interventions. The majority of existing security awareness approaches aims to change behaviour through the use of training (Puhakainen, 2006:54). Most of the research that does propose training has two shortcomings: no underlying theories presented and insufficient empirical evidence on the practical efficiency of methods (Puhakainen, 2006:54).

One school of thought attributes changes in behaviour to the result of changes in environmental variables because of undesirable behaviours. For example, abuse of computer systems by employees may be countered by disciplinary actions against those employees. So the use of measures to alter behaviour is used, such as punishment and reward for certain security practices (Puhakainen, 2006:55). An example of this research is the work carried out by Straub (1990). Behavioural security is also concerned with what motivates security-related behaviours. The research of Pahnila et al (2007), for example, undertakes to explain and provide evidence as to why people do not comply with security policies and what it is that influences such behaviour. They developed a model to explain this and provide an insight into the determinants of behaviour.

The next chapter will show that there is an inadequate understanding by practitioners on the various security approaches for security awareness; what works well and what does not. The existing research, by and large lacks credibility. This is apparent by the security awareness approaches discussed by scholars without empirical evidence supporting their practical effectiveness (Puhakainen, 2006:30). The only empirical evidence that does exist (with respect to information security awareness research) shows the practical effectiveness of deterrence. Further empirical evidence showing the effectiveness of security awareness training or awareness campaigns is not available, even though the effectiveness of training and campaign activities has been shown in other fields (e.g. in cases where AIDS training has been a successful intervention) (Puhakainen, 2006:69,139).

Furthermore, scholars have pointed out that only a few existing studies are theoretically grounded (Puhakainen, 2006:149; Pahnila et al., 2007) and more work is needed in this regard. Unless explicitly mentioned, all the research mentioned in the next chapter lacks a theoretical basis. Security awareness research in this context can be categorised as follows: conceptual models providing practical guidance for security awareness, theoretical models without empirical support and theoretical models with empirical support (Pahnila et al., 2007). Puhakainen (2006:56) found only seven studies out of 59 that showed a theoretical foundation.

In an attempt to address the shortcomings and limitations of existing research, Puhakainen (2006) developed three design theories to explain and improve IS behaviour. One of the design theories for IS awareness training was tested in two organisations. The research showed that the developed theory was relevant for developing practical security awareness training programmes. The researcher relied on the feedback from users, their colleagues and what they observed to determine the effectiveness of the security awareness training programme. This programme was shown to achieve positive results, change user attitudes and make users more conscious about their behaviour. The author calls for more practical studies in this regard (Puhakainen, 2006:106, 114, 139).

However, Puhakainen’s (2006) work has the following limitations. Direct observation was not used, instead anecdotal evidence from the organisation’s manager, interviews and discussions with employees and “participatory observation” were relied upon, which are susceptible to the subject-expectancy effect. Ultimately, the research was reliant on user behaviour feedback and Puhakainen admitted that the research results were based on the researcher’s interpretation – someone else may have come to a different conclusion (Puhakainen, 2006:107).

Kruger, Drevin and Steyn (2006) recommend that system data also be gathered to supplement employee surveyed data. For the purposes of research it may not be necessary to link specific individuals to specific data thus avoiding any ethical concerns that may be raised. They also attempt to list potential system data that would be captured for each security area. While this is a good idea, the feasibility and usefulness of this information is not discussed. More work should be done in this regard, that is, more detail should be provided including the type of data that should be focused on instead of just referring to “system data” and “e-mail system logs”. The researchers plan to determine the applicability of this system data in future research work.

Many of the existing studies (such as those carried out by Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2007) are limited by certain factors such as the research being carried out in a lab environment, simulating phishing sites (e.g. assessing participants’ ability to identify phishing websites without showing them the phishing email messages that would typically take someone to such websites). In addition, the participants involved were more educated and younger than the general Internet user population (typically university students) so the results may not be generalisable to other groups.

Scholars (such as Srikwan & Jakobsson, 2007) call for educational efforts to demonstrate and place emphasis on the link between behaviour and the outcome of that behaviour. They want users to understand not only what they must do but why.

Srikwan and Jakobsson (2007:5,6) also contend that some examples of educational movies are highly technical in nature, implying they are not suitable for the layperson. This research on the other hand is aimed at lay people who have a basic understanding of computer usage and as such will not suffer from the same problems that the previously mentioned example does.

Some researchers have made use of computer games as a security awareness tool, such as Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong and Nunge (2007). Although it has been shown that these mechanisms may be successful in helping people for example identify phishing attacks, this kind of training may have limited flexibility in terms of being able to convey various security messages and subtleties.

This research report builds on existing behavioural information security research, puts forward a theoretical model explaining how learning takes place and then tests the model empirically. Scholars have called for research showing the effectiveness of awareness training since existing research material does not adequately answer questions of awareness efficacy. To summarise, the following limitations are present with the existing research:

- lack of empirical evidence on the efficacy and appropriateness of using certain awareness mechanisms
- lack of a theoretical foundation for most research work
- lack of direct observation studies of security behaviours
- inadequate/ineffective learning and educational principles used in security awareness techniques
- susceptibility of much of the research methodologies to the subject-expectancy effect
- neglect of some security topics (e.g. mobile computing risks) while others are emphasised (e.g. phishing threats)
- inadequate research on the role that internalised knowledge plays (of awareness material)

1.3. INTRODUCING A VIABLE RESEARCH DESIGN

The purpose of this section is to provide the reader with a high-level overview of what methods were used to achieve the objectives of this report. A detailed discussion of the design is presented in Chapter 3.

1.3.1. Hypothesis

There seems to be a link between awareness activities and employee behaviour with respect to information security. Human action or inaction is seen to influence information security. For example, Stanton et al. (2005:125) argue that appropriate constructive behaviour by end-users and administrators improves information security, while inappropriate behaviours can substantially inhibit it.

But how do awareness activities affect information security behaviour? Based on the weight given to awareness activities by researchers and standards bodies mentioned above, one would expect exposure to awareness activities by end-users to have an influence on their behaviour and thus the security character of an organisation.

It is intuitively appealing to believe that more awareness leads to better security behaviour. What is required is a theoretical basis for explaining why we would expect exposure to awareness training would lead to better security behaviour.

The theoretical foundation of this research work is based on the work by Nonaka and Takeuchi (1995:61) who argue that there are two types of knowledge and both are needed to help explain organisational learning, that is, tacit knowledge and explicit knowledge. The hypotheses presented below are based on this model. The theoretical foundation is discussed in further detail in Chapter 2.

1.3.2. Variables

The variables involved in this research are described below.

1.3.2.1. Hypothesis 1a, 1b, 1c

The dependent variable is information security behaviour. The first step in measuring security behaviour is to obtain a consistent definition of information security behaviour. Stanton et al. (2005:126) developed a taxonomy of security behaviours mapped across two factors, namely level of technical expertise (either high or low) and, intentions (either malicious, neutral or beneficial). The taxonomy resulted in six categories of security behaviours that have been shown to cover most information security behaviours. The taxonomy is shown in the table below:

Table 1: Two-factor taxonomy of security behaviours (Stanton et al :2005)

Expertise	Intentions	Title
High	Malicious	Intentional destruction
Low	Malicious	Detrimental misuse
High	Neutral	Dangerous tinkering
Low	Neutral	Naïve mistakes
High	Beneficial	Aware Assurance
Low	Beneficial	Basic hygiene

This research focused on security behaviours requiring low technical expertise. This is because of the complexity and lack of instruments to measure high technical expertise of individuals reliably and consistently. Consequently the security behaviours with malicious, neutral and beneficial intentions requiring low technical expertise were measured in this research and constituted the dependent variable.

The independent variable consisted of a set of security awareness exposures where participants viewed an awareness movie and completed a test afterwards in three parts. This movie is based on the organisation's acceptable usage policy (AUP).

Therefore the following hypotheses were tested:

- **H1a: Naive mistakes (neutral intent):** End-user exposure to security awareness training on appropriate information handling improves secure handling of information.

- **H1b: Detrimental misuse (malicious intent):** End-user exposure to security awareness training on acceptable usage of Internet facilities diminishes Internet abuse by end-users.

- **H1c: Basic hygiene (beneficial intent):** End-user exposure to security awareness training on password management best practices improves secure handling of passwords by end-users.

1.3.2.2. Hypothesis 2

As with Hypothesis 1, the independent variable for Hypothesis 2 consisted of security awareness training. However, the dependent variable is the level of internalised knowledge obtained from the training. In other words, to what extent does the training (explicit knowledge) lead to an internalisation of the material presented (tacit knowledge)? The following was tested:

- **H2:** End-user exposure to security awareness training increases the internalisation of security knowledge;

1.3.2.3. Hypothesis 3

The independent variable is explicit knowledge made implicit (internalised knowledge). The dependent variable is information security behaviour, as in hypothesis 1. Therefore the following was tested:

- **H3:** Internalised security information is necessary for users to enact appropriate security behaviours.

1.3.3. Method/research design

A case study was carried out in an organisation consisting of a population of 5,726 employees. In order to draw the sample, stratified random sampling was used (Welman & Kruger, 2001:55–56).

An experimental and a control group were used. The experimental group were exposed to security awareness training. Both groups were required to write a short test that assessed their level of understating of the material presented. This was required to test hypothesis 2, that is, it is expected that those who pass the test will be more likely to enact the appropriate security behaviours. After the end-users have been exposed to security awareness training, on-the-job security related behaviours (confirmed by previous research carried out by behavioural information security researchers) was observed for both the experimental and the control groups.

1.3.4. Validity

The research approach recognised and then controlled threats to internal validity of the research, that is, showing unequivocally that exposure to security awareness training directly influences on-the-job security behaviours or not, and whether internalisation of security knowledge influences these behaviours. The nuisance variables controlled were corporate culture, intelligence, socioeconomic status, commitment to the organisation, status in the organisation, educational level, tenure and previous exposure to security awareness training. According to Welman and Kruger (2001:73) the most practical way to control nuisance variables is through the use of a control group in conjunction with random assignment of end-users to control and experimental groups.

Obviously, a great deal is expected from users during awareness initiatives, that is, their time and attention, as well as expecting them to absorb the message. This research used a novel approach to convey the message to end-users that was both entertaining and not technically focused. Since direct observation of the participants took place, problems that some surveys suffer from, such as the subject-expectancy effect, were eliminated. PayPal (Can you spot phishing – Paypal, 2008), for example, provides an online questionnaire for users to test their understanding of phishing threats and how they work. Unfortunately this does not measure users' real-world behaviour as, for example, the work carried out by Whalen and Inkpen (2005) does. SonicWALL has a more realistic and useful "Phishing IQ test" that provides users with sample emails and they have to decide whether these are legitimate or not (SonicWALL, 2008). Anandpara, Dingman, Jakobsson, Liu and Roinestad agree, stating that the multitude of studies which perform general evaluations of phishing vulnerabilities largely neglect the subject-expectancy effect. According to Anandpara et al. (2007:3) there have been no previous attempts to gather any empirical data on the effectiveness of these phishing IQ tests.

This research report supports the argument of demonstrating a link between behaviour and the outcome of that behaviour, since the policies and security requirements were conveyed to the participants through a customised movie developed for the organisation. The movie script initially showed the unwanted behaviour and its consequences. Thereafter the correct behaviour is demonstrated by the actors and the outcome of this is also shown. In addition, the movie avoids technical issues that may confuse the user. In fact, scholars contend that using a movie format to communicate security risks to users seems to offer considerable benefits (Mitnick & Simon, 2002; Srikwan & Jakobsson, 2007:5). Using this format also addresses some of the concerns raised by scholars such as Kovacich and Halibozek (2003:258) and Lafleur (1992:4) about overcoming the resistance to awareness by employees and getting users to pay attention to awareness material (Kumaraguru et al, 2007a).

The advantage of using a movie in this research is that it is not limited to a specific demographic as an interactive game (used by other researchers) would be, for example. The added advantage of using a movie in this research is the fact that the message is not only reliant on language but also on the actions of the characters, thus not being constrained to the interpretations of language. Users must understand not only what they must do but why (Sheng et al., 2007:5).

1.3.5. Data collection and measuring instruments

Information security behaviour is a construct and is measured indirectly by measuring specific behaviours requiring low technical expertise. By using multiple indicators of information security, irrelevant constructs are minimised. The construct validity of information security behaviour (dependent variable for hypotheses 1 & 3) is further maximised since direct observation is used as a measuring instrument. In addition, more than one measure is used to measure security behaviour (Welman & Kruger, 2001:136). Therefore, factors such a faking, measurement reactivity and socially desirable responses are eliminated.

These behaviours were measured before and after security awareness training took place. Through investigative techniques, measures such as the strength of passwords used by participants and handling of sensitive information were observed and scored. Thus the researcher assessed the behaviour of the participants.

Instruments used to measure these security behaviours are discussed in detail in Chapter 3.

This research will therefore help to answer the following questions:

- Does end-user exposure to information security awareness training affect end-user security behaviour (whether neutral, beneficial, or malicious)?
- What are the implications for organisational awareness training programmes arising from a better understanding of the role of security awareness training on behaviour?
- Does end-user exposure to security training increase the internalisation of security knowledge?
- Does internalised knowledge of security policies lead to users enacting correct security behaviours?

In Chapter 2, the information security awareness landscape will be introduced and classified. A broad review of studies on information security awareness is undertaken and their limitations, weaknesses and areas for improvement are discussed. In addition the theoretical foundation of this research is presented.

Chapter 3 presents the research design in detail that was introduced above. Each research strategy will be explained with respect to sampling, data collection and analysis. The rationale of the strategy is also discussed.

Chapter 4 presents the results of the implemented research strategies described in the previous chapters. For each strategy, the results of the sampling, data collection and data analysis sections are presented. Essentially the results of the statistical techniques used to test the research hypotheses are described here. This chapter also builds on the outcome of the statistical techniques performed in Chapter 3. The results of these techniques are interpreted in light of the hypotheses and the literature survey presented in Chapter 2. The implications for the results for scholars and practitioners are examined.

Chapter 5 is a conclusion of the research undertaken. An overview of the study is presented and a summary of the results is presented. A research agenda and recommendations are presented for practitioners and scholars to follow. The chapter concludes with an explanation of the limitations of this research.

Two appendices are provided in this research report. Appendix A is an extract of the Acceptable Usage Policy of the organisation in question. All the awareness material discussed in this report is based on this policy. Appendix B consists of three security tests that were undertaken by the control and experimental group end-users during the awareness training initiative.

1.4. SUMMARY

This chapter firstly introduced the importance of information security awareness in the lives of scholars and practitioners. It demonstrated that there is a shortage of in-depth research showing the practical effectiveness of information security awareness initiatives and their impact on end-users behaviour. The role that individuals play in information security is significant and needs further research. Understanding the nature of such a relationship will be particularly helpful to organisations as they are ultimately dependent on people to ensure that their security systems are implemented and managed on a sustainable basis.

There are also financial (and non-financial) implications for organisations that do not ensure that security is maintained, as reported by various security surveys. Organisations are particularly at risk of data theft and financial fraud by employees of their organisation who are familiar with organisational processes and systems. Given the gaps in the existing research literature and calls by researchers for further research the subsequent research design was introduced.

This research examines the effect of information security awareness training on security related behaviours. A case study of an organisation was undertaken to determine whether exposure by employees to security awareness training improves their security behaviour at work. This is determined by directly observing employee on-the-job behaviour before and after security awareness training. In addition, the degree to which the training is internalised and its subsequent effect on employee behaviour was also examined as a factor that influences security behaviour.

Finally, the outcome of this study will provide a set of tools or techniques that future researchers can use to measure user behaviour. Learning principles which have been called for by previous scholars have been employed to ensure maximum effectiveness of the awareness initiatives. For example, previous research has highlighted the need to demonstrate exactly what behaviour is required, the consequences of not behaving correctly and the need to ensure that immediate feedback is given in non-compliant situations.

CHAPTER 2 : THE INFORMATION SECURITY AWARENESS LANDSCAPE

While good user education can hardly secure a system, we believe that poor user education can put it at serious harm.

Srikwan & Jakobsson (2007:1)

2.1 INTRODUCTION

The purpose of the chapter is to demonstrate that the research question presented in this report has not been replicated before and to present a theoretical framework upon which this study builds and extends. This will be done by identifying, analysing and discussing arguments identified in this literature survey. Specifically, this chapter will achieve the following outcomes: show that the question of the impact of security awareness training on security behaviour has not been adequately answered by previous research; show that some authors have explicitly and implicitly called for further research in this regard; demonstrate that such research is worthwhile and necessary and will contribute significantly to the information security community; and show that, information security awareness efforts can be beneficial. The hypotheses introduced in the previous chapter will be tested in Chapter 3.

The aim of this literature survey is not to reflect every paper published on information security awareness, but rather to reflect the state of this area of research, trends in this area, and shortcoming or limitations in the existing literature. I therefore feel confident that the material presented is adequate, appropriate and effective in achieving the outcomes of this literature survey as mentioned above. This literature survey was conducted by reviewing the foremost information security and IT journals. This was done with the aid of electronic database journals, such as ACM, Emerald, JSTOR, Science Direct and Springer, which greatly assisted me in obtaining the necessary material. In addition, the use of Google Scholar was of great help in identifying journals and sources of citations. In addition, information security-related conference proceedings were also used extensively.

IT systems are dependent on people. Schneier (2003:10) maintains that information security is more about behaviour than anything else, that is, getting people to behave in a certain way. It is people's intentional and unintentional actions that cause adverse consequences that security wants to prevent. Schneier wrote about this in *Secrets & lies* (2000), in which he says that one of the reasons for the book was to correct the notion put forward from his previous book that cryptography was the answer to security. The principle he is pointing out is why an attacker would spend time and money trying to break an encryption algorithm, for example, when they could more easily bribe an employee who has been explicitly given access to the information required for their day-to-day activities. Despite the hype from vendors about the need for security products many critical security activities have not and cannot be automated. This means that organisations are dependent on people to achieve a secure environment. Since humans are seen as the "weakest link" in the information security chain (Schneier, 2000; Stanton et al. 2003:1; Katsikas, 2000:130; van Niekerk & von Solms, 2004:2; von Solms, 2000:618; Kabay, 2002:35), there is a clear need to ensure that users are trained correctly in terms of information security policies. The goal is to ensure that users use the necessary policies and to ensure that they are not misused or misinterpreted, thereby ensuring the effectiveness of policies (Siponen, 2000a:31) and efficiencies of security processes. Incorrect security behaviour must be addressed as it is the major reason for inefficient security measures (Vyskoc & Fibikova, 2001).

Users need to understand why security must be taken seriously, the benefits to them personally (i.e. what they gain from this) and how this will assist them in carrying out their job (Peltier, 2000:23). Further, users should be given the opportunity to review and accept the necessary policies (Markey, 1989:85). Security awareness efforts are seen as the "first line of defence" (OECD, 2002:10). On the other hand, Van Niekerk and von Solms (2004) argue that awareness initiatives, while necessary, are not sufficient to obtain the desired results, while other authors simply consider educating users futile (Nielsen, 2004; Ranum, 2005; Evers, 2006).

To this end, this chapter will carry out a literature survey on the available research. Initially, the phenomenon of information security awareness will be examined, including the main themes of information security research carried out thus far: the importance of the research as stated by researchers and various awareness techniques recommended. Related topics covering computer abuse and insider threats will also be discussed. A discussion of a theoretical model and how it can be used for information security awareness initiatives will be presented. Next, significant work done in the relatively new field of behavioural information security will be examined and discussed. Finally, this chapter will argue why this research work is both worthwhile and necessary.

2.2 INFORMATION SECURITY LEARNING

Before proceeding it is worthwhile to get an understanding of the meaning of information security learning. According to the National Institute of Science and Technology (NIST) security learning is on a continuum with "awareness" at the one extreme followed by "training" and with "education" at the other extreme (See Figure 1 below). Generally the nature of learning becomes more detailed and comprehensive as one moves across the continuum (NIST, 1998:14). Security awareness is directed at all employees in an organisation and is primarily aimed at getting employees to focus on security matters using attention-getting techniques (Schlienger & Teufel, 2003; NIST, 1998:15, Hansche, Berti & Hare, 2004:54), so that they are able to recognise security incidents and respond accordingly as required. The employee is regarded as a passive receiver of information (NIST, 1998:15, Hansche et al, 2004:54). Training on the other hand is concerned with continued teaching of security skills to groups other than IT security staff. For example, teaching web application developers how to code securely is considered training according to the NIST definition. Education is focused instruction for information security personnel on all aspects of the multidimensional Information Security discipline.

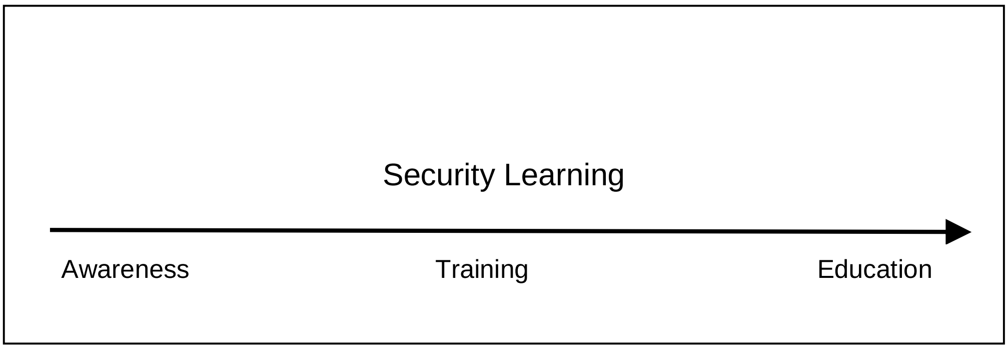


Figure 1: Security Learning Continuum (adapted from NIST, 1998)

Hansche et al. (2004:54) provide some clarity on what security awareness initiatives are and why they are required. The basis of their argument is that all users must understand the policy and apply good security habits when carrying out their duties. This is because it is believed that information security incidents are often as a result of inattention on the part of end-users (Hansche et al., 2004:56). The initiatives are a way to "raise the security consciousness" of employees as some may not be aware of the consequences of their actions, they believe (Hansche et al., 2004:55).

The importance of the human element has come to prominence in the research community recently, prompting a number of research activities. According to Puhakainen, the existing body of research in this regard can be categorised into two distinct areas. The first area considers security awareness to mean attracting end-users to IT Security issues, while the second approach regards IT Security awareness to mean users' understanding IT security and binding themselves to it. Consequently, their awareness increases as their attitudes and behaviours change thus causing them to secure organisational resources (2006:9–10). However, as will be shown below, most of these approaches lack a theoretical underpinning and verified results to prove the effectiveness of security awareness. This is important as practitioners need to understand why a particular approach is expected to have a certain affect and adds to the credibility of the particular approach chosen by a practitioner (Puhakainen, 2006:10).

Puhakainen (2006:89) says that the difference between security awareness training and security awareness campaigns can be open to interpretation. They both want to achieve sustainable attitudinal and behavioural improvements towards policies in end-users. The difference (according to Puhakainen) is that security training is goal-directed learning through lessons which teach the skills and knowledge needed to comply with IS policies. Security awareness campaigns are a method to market IS through persuasive information-sharing techniques (2006:89). This research report adopts this definition of security awareness.

It is well accepted that measuring the effectiveness of any awareness programme is key. Hansche et al. (2004:69) provide some insight into how this should be done. They believe that informally checking behaviours and attitudes should be sufficient and recommend the following to security practitioners:

- password cracking
- obtaining anecdotal evidence by speaking to people at pause areas
- tracking the number of incidents reported (before and after)
- clean desk audits
- tracking of who has reviewed security material (such as policies)
- distributing surveys or questionnaires in order to get input from employees. For example, following up to see what employees remember and what worked.

Although this approach is supported by many scholars (e.g. Kruger et al., 2006; and see the following sections), a more scientific approach is needed since current methods of measuring effectiveness of awareness initiatives are not adequate to determine the effectiveness of security awareness training. As Hansche et al. themselves state, the measurement must show whether the original objectives have been met (2004:70). It is also important to ensure that the goal of the security awareness message is clear from the start. The goal of any awareness initiative is to ultimately have an effect on behaviour or at least try to do so.

2.3 THEORETICAL FOUNDATION

Since one of the aims of this chapter is to show that the hypotheses in this chapter are reasonable, the theoretical foundation upon which this research is based will initially be introduced. Thereafter, the hypotheses introduced in the previous chapter will be revisited in light of the objectives of this literature survey.

The theoretical foundation of this research work is based on the work by Nonaka and Takeuchi. They contend that the main reason why Japanese companies excel is because they are good at "organisational knowledge creation", that is, the company creates new knowledge, disseminates it, and has it reflected in new products, services and systems (1995:3,4).

Drucker maintains that individuals do and will play a pivotal role in society (2003:7). In organisations individuals create knowledge. Organisations are dependent on individuals for this since they cannot create knowledge. What organisations can do is magnify the knowledge created by individuals and make it meaningful across the organisation thus creating a knowledge creation process (Nonaka and Takeuchi, 1995:59).

Nonaka and Takeuchi (1995:61) argue that there are two types of knowledge and both are needed to help explain organisational learning, that is, tacit knowledge and explicit knowledge. They explain that the way an organisation learns is by oscillating between the two types of knowledge. Tacit knowledge is not tangible and is subjective since it is that which is possessed by employees of an organisation. This includes individual beliefs, experiences and understandings of the organisation and what the organisation requires from them. Tacit knowledge also includes the notion of mental models – it is how individuals view reality now and how they envision it in the future. Tacit knowledge by individuals is the basis for organisational knowledge creation (Nonaka & Takeuchi, 1995:60).

Explicit knowledge, on the other hand, is codified, formal and easily expressed. Examples of explicit knowledge include organisational policies, pamphlets, directives and systems. Westerners emphasise explicit knowledge, while the Japanese emphasise tacit knowledge. Nonaka and Takeuchi, however, are of the opinion that these types of knowledge are not separate and are actually complementary. The vital assumption of knowledge creation is that human knowledge is produced through the social interaction of explicit and tacit knowledge which occurs between individuals. Therefore organisational knowledge creation spirals out from individuals across departmental, divisional and organisational boundaries (Nonaka & Takeuchi, 1995:61, 72).

Thus the key to knowledge creation is the conversion of tacit knowledge to explicit knowledge in an organisation, and when the interaction between tacit and explicit knowledge is elevated dynamically from a lower organisational unit in the organisation (e.g. a small business unit) to higher levels in the organisation (e.g. divisional level or organisation wide). The theory proposed by Nonaka and Takeuchi is based on four modes of knowledge conversion (a dynamic and continuous interaction between tacit and explicit knowledge), which are in actual fact "the engine" of the knowledge-creation process. Each mode produces different outputs. It is this process of knowledge building that this research report focuses on. The hypotheses presented in this report are based on these knowledge creation processes (Nonaka & Takeuchi, 1995:57,70).

The learning path in an organisation follows four cyclical stages (Nonaka & Takeuchi, 1995:70, 71):

- Employees share tacit knowledge.
- Tacit knowledge is made explicit by formalising it (e.g. policies).
- Formalised knowledge is disseminated (e.g. awareness activities).
- Employees "learn by doing" and thus explicit knowledge is made tacit by employees internalising the explicit knowledge. The cycle then starts from stage 1 again and forms an infinite loop.

This research report proposes a theoretical model to help explain how awareness training influences behaviour. Since security is dependent on human behaviour it makes sense to have a proper security awareness programme that takes this into account. Employees are often the greatest source of security breaches mostly as a result of their ignorance.

It is further proposed that in order to ensure appropriate security behaviour, employees need explicit knowledge of security policies and tacit knowledge on how to enact the appropriate security behaviour. This research report therefore argues that future security awareness programmes must take explicit and implicit knowledge into account.

Figure 2 below puts the model described above in context and shows the actual mechanisms that were tested. Firstly, users undergo security awareness training (1). This is in the form of security awareness material showing correct and incorrect behaviours to which users are exposed. Thus the security message is made explicit and disseminated to users (2). As argued above, explicit knowledge also needs to be made tacit by users internalising it. So, after the awareness material has been presented, users were required to write a short test that measured to what extent the message had been internalised (3). Thereafter, the actual behaviour of respondents were measured to test whether their actual behaviour has changed as a result of the awareness training (4) and, whether internalised knowledge (comprehension) is needed for appropriate behaviour (5).

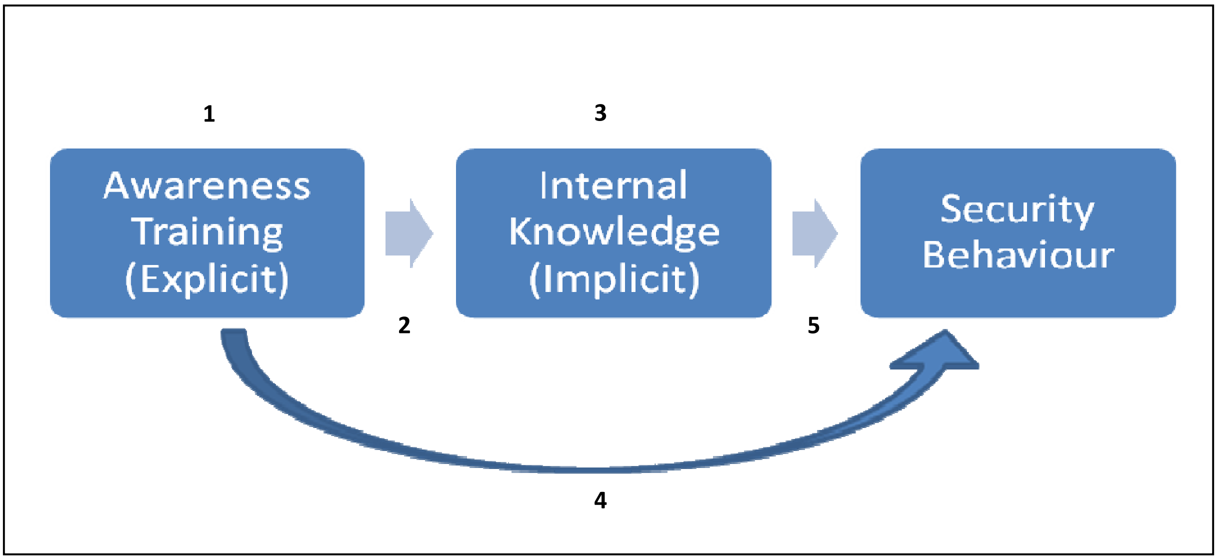


Figure 2: Theoretical model explaining the way in which security awareness training affects behaviour

2.4 PREVIOUS RESEARCH HAS NOT ANSWERED THE RESEARCH QUESTION

Research carried out on information security has traditionally been slanted towards technical aspects of security (Siponen, 2001:24; Stanton et al., 2003:1; Trompeter & Eloff, 2001:384), typically rooted in computer science and mathematics. Security was traditionally seen as a service to be provided and not something that was influenced by users. However, it was soon recognised that focusing on technical issues alone is inadequate (von Solms, 2000: 615; Schneier, 2000:xi). Technologies meant to provide security ultimately depend on the effective implementation and operation of these technologies by people. Many authors then argued that since "insiders" (personnel) pose the greatest security threat to an organisation, it follows that appropriate behaviour must be encouraged in order to enhance the organisation's security position (Janczewski & Xinli, 2002:179; Leach, 2003:685; van Niekerk & von Solms, 2004:2; Stanton et al., 2005:125; Pahnila et al, 2007). Information security awareness is needed to educate users and continually remind them of new threats, with the objective being to change the behaviour of the user (Thomson & von Solms, 1998:168). Awareness of policies is needed by all individuals in an organisation to ensure that policies are well understood. Users need to be aware of security requirements in order to ensure that the value of security policies are not lost (Puhakainen 2006:4).

Various branches relating to information security awareness research currently exist. The landscape of information security awareness research can be categorised as follows:

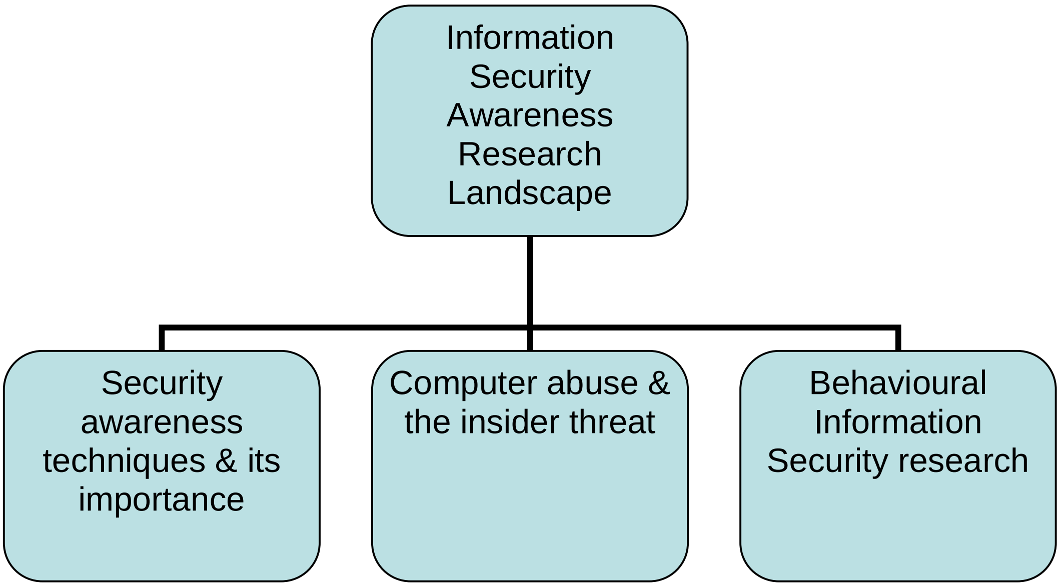

Information Security Awareness Research Landscape
Security awareness techniques & its importance
Computer abuse & the insider threat
Behavioural Information Security research

Figure 3: Information security awareness landscape

Figure 3 demonstrates one way of making sense of the available information security research. Most of the research work can be placed into one of these categories.

2.4.1 Research about security awareness techniques and its importance

Bray promotes the use of security awareness as a way to avoid security breaches. He repeats the old adage that a combination of people, process and technology is required (2002:11). Bray provides some practical guidance for security awareness for practitioners to follow.

Most of the research falls into this category and concentrates on the importance of awareness initiatives (Nosworthy, 2000; Furnell, Gennatou & Dowland, 2000; von Solms, 2000; von Solms, 2001; Siponen, 2001; Janczewkski & Xinli, 2002) and awareness techniques (Furnell, Sanders & Warren, 1997; Gaunt, 1998; Gaunt, 2000; van Niekerk & von Solms, 2004; Trompeter & Eloff, 2001; Katsikas, 2000; Johnston, Eloff & Labuschange, 2003; Thomson & von Solms, 1998; Cox, Connolly & Currall, 2001; Denning, 1999; Furnell et al., 1997). Some of this research, is not necessarily based on a theoretical model, but instead simply provides guidance on what methods to use. Sommers & Robinson (2004:379) show how an awareness video and a quiz can be used to train students at a university. However, the researchers admitted that they had no way of measuring the effectiveness of this intervention. A video was simply shown and respondents were required to take a quiz afterwards. McCoy and Fowler (2004:349) also deployed a security awareness campaign at a university campus. They too, however, did not use any metrics and found that measuring effectiveness of security awareness training to be a difficult task to carry out – thus implying the importance for this piece of research. Other researchers have also demonstrated techniques for information security awareness programmes such as Perry (1985:94–95), Spurling (1995:20) Parker (1998:466), Cox et al. (2001:12), Desman (2002:x), Kovacich (1998:113) and Markey (1989).

In addition, well-established security management standards, such as SABS ISO/IEC 17799 and the OECD guidelines, for information systems security all promote the importance of making people aware of security awareness issues. The question one has to ask is to what end? In other words, does making users more aware lead to more secure behaviour, or are awareness campaigns doomed to fail (Stephanou & Dagada, 2008)? This research will show that there is a shortage of in-depth information security awareness research to answer these questions (Siponen, 2001:24). In addition, behavioural concepts are not properly taken into account for security awareness programmes (Van Niekerk & von Solms, 2004).

Barman's (2002:32) approach talks about how to write and implement security policies. In order for implementation to succeed the significance of information security awareness training should be focused on and should be mandatory. End-users need to understand what the policies say and their roles as employees in these policies. The use of punishment is advocated and encouraged (e.g. withholding salaries until training has been completed). Furnell et al. (1997:708) argue that employees need to know, understand and accept the necessary security requirements from the organisation. They also advocate the use of punishment as a means of enforcement. Gaunt (1998:134) also advocates punishment in a sense by stating that employees should be denied access to information systems until they have undergone information security awareness training. He offers concrete means to achieve security awareness - such as ensuring that employees' conditions of employment include security requirements. Gaunt (2000:154) says that users should also participate in the development of policies. Not only are end-users important but management must also be targeted. Katsikas (2000) argues for the need for management to be trained and then puts forward a methodology for determining training needs. He stresses that it is important that individual needs must first be assessed for training purposes.

In the 2007 Computer Security Institute (CSI) Survey, it is reported that there is a substantial increase in the importance of security awareness as perceived by those surveyed. For the first time in the survey's history, respondents were also asked how they measure the effectiveness of their own awareness initiatives. Results of this survey may provide further insight into the success of security awareness initiatives.

In the 2006 CSI survey, on average, respondents felt that their organisations were under-investing in awareness at that time (Computer Security Institute, 2006). These results imply that organisations do realise the importance of security awareness efforts. Thus the need for information security is well established, but there is inadequate research on the behavioural aspects of awareness initiatives (Siponen, 2001:24; Schultz, 2004:1; Van Niekerk & von Solms, 2004; Srikwan & Jakobsson, 2007:2).

2.4.1.1 Problems with current awareness techniques

Despite the understanding that awareness is important, it is unclear whether a clear message is being communicated to users in the first place (Gaunt, 2000:152-153). This is especially true for dynamic, complex threats such as phishing attacks. Srikwan and Jakobsson (2007), for example, doubt whether a clear message is being communicated to users with respect to identity theft threats, specifically on what to do and why it must be done. This is despite a vast amount of guidance on this subject being directed at users. South African banking clients, for example, are frequently warned about the threats of phishing scams (via email, SMS and so on). Are these interventions having an effect? Perhaps there is too much information for lay people to digest and security practitioners may be unwittingly shooting themselves in the foot. For example, the research by Anandpara et al. (2007) shows that even though users underwent security education on phishing, the result was not an improvement in the ability of participants to identify phishing scams, but rather to make participants more suspicious or concerned, which was the only measurable effect.

There are other obstacles to training such as human resistance to awareness training, which some believe is the main obstacle to effective training (Kovacich & Halibozek, 2003:258) and thus their full cooperation is required. This resistance to secure behaviour can be overcome simply by using an information security awareness programme: promotional component (publications) and an interactive component, for example briefings (Lafleur, 1992:4). Lafleur (1992:4–5) seeks to explore the human characteristic of resistance to change and seeks to understand human behaviour in order to overcome this resistance.

Does making users more aware lead to more secure behaviour and therefore contribute to a more “secure” organisation? This is particularly pertinent given the increase in users that fall prey to phishing attacks (Anandpara et al., 2007:1). One reason why users fall for phishing attacks might be because we do not have a detailed understanding of the many guises that attacks might take or the technical sophistication needed to identify a false email for example. This is mainly due to the fact that most users see security as secondary and ignore risks as they are not constantly looking for them (Anandpara et al., 2007:2).

So, even though methods may be used to make users aware, recipients of the security awareness message may not apply what they know whether they understand the message or not. Some of the reasons for this are because security technologies are difficult to use and consequently not used very well. For example, Furnell (2005:274) demonstrates the difficulty that users have in finding, understanding and using security features in Microsoft Word. In another case, Whalen and Inkpen (2005:137) measured eyeball tracking of users when using web browsers and concluded that although some security information is viewed (indicating that users were "security aware"), users do not interact with it in order to fully understand its implications. The study also found that users tend to stop looking for security information once they have logged into a site (Whalen & Inkpen 2005:143).

The problem may be more complex than originally anticipated by security practitioners. Perhaps the solution is not only to deploy awareness campaigns and educate users, but more related to the notion of the ability of users to understand risk and make trade-offs (Schneier, 2003:17). In addition, attackers take advantage of personnel being naturally helpful in order to subvert a system (Mitnick & Simon, 2002). Most of the time people are told what to do without explaining why they need to do this. This is linked to people's understanding of threats. If they are able to understand the underlying threat then they will be able to look for patterns and consequently mitigate any threat posed (Srikwan & Jakobsson 2007). Cox et al. echo this, arguing that not only should employees understand policies but organisations must help them to understand security issues (2001:12). Their research proposes methods for increasing awareness in an academic setting.

Although it is established that awareness is important, Srikwan and Jakobsson (2007) argue that the effectiveness of secure online education is inadequate. Traditional security awareness efforts also seem to have inadequate results as witnessed by various news reports documented in the previous chapter. Srikwan and Jakobsson (2007) argue that educational efforts generally expect too much from the audience, while some people – in an effort to make the message more palatable – simplify the message to such an extent that the meaning is diluted.

Without an adequate understanding of security requirements and their support, security processes are bound to be ineffective (Van Niekerk & von Solms, 2004). For example, a well-crafted incident management process is useless if an employee is not aware of firstly what a security incident looks like and then how to respond to the incident when one is recognised. Ultimately, security education in this context becomes inadequate. Thus security awareness practitioners need to ensure that there is a connection made between what a user knows and what the appropriate behaviour expected from them is. In order for security to be enhanced they need to be told not only what to do but why they should do it. Murray (1991:204) holds that employees may not understand the inherent risks in their actions and thus security problems are as a result of their incompetence. In order to overcome this problem the use of security awareness programmes is supported.

Security education may inadvertently also have the opposite effect intended and enhance the level of risk that users expose themselves to. For example, if users are instructed explicitly not to share their credit card details with anyone requesting them via email and the attack is changed so that this information is requested telephonically, then users could be at risk for simply doing what they were told to do. In essence the message needs to be simple enough to capture the problem without losing the complexity of the threat. This is particularly true for education about phishing attacks (Srikwan & Jakobsson 2007). Another case in point is the research carried out by Anandpara et al. (2007) mentioned above.

Throughout this research report it will become apparent that some security topics are neglected (Srikwan & Jakobsson 2007), while others are emphasised. For example, people are not told that they could unintentionally introduce malicious codes onto their computer by installing a seemingly innocuous program. Thus security awareness practitioners need to ensure that there is a connection made between what a user knows and what the appropriate behaviour expected from them is. In order for security to be enhanced they need to be told not only what to do but why they should do it.

The other challenge with security education is to ensure that users actually use the material that is available. Some researchers have considered educating users futile (Nielsen, 2004; Ranum, 2005; Schneier, 2006; Evers, 2006), and it was mentioned previously that generally getting the correct message across can be difficult.

2.4.1.2 Alternative awareness techniques

Despite the challenges with security education as mentioned above, Kumaraguru et al. (2007a) proved that security awareness material – when used – may be effective. They found that online material that informs users about the threats of phishing was highly effective and that it resulted in an improvement in the ability of users to identify phishing sites. Kumaraguru et al. also surmise that the reasons why it is believed that teaching users about phishing attacks is not effective are twofold: Firstly, it is believed that it is difficult to teach users complex security issues and, secondly, since users perceive security to be of secondary importance they do not pay enough attention to it (2007a). Their research demonstrated that it is possible to overcome the first reason – by teaching users simple principles the users were able to identify most phishing scams. The second reason could be overcome by devising unique ways in which to deliver the message to the user and to ensure that their attention was held. These researchers also call for investigations into more effective techniques for delivering the awareness message, inducing users actually to read and to absorb the material and to ensure that more research which examines the quality of awareness materials presented is conducted. Srikwan and Jakobsson (2007), for example, call for the behaviour of end-users to be emphasised in awareness campaigns. Despite the positive results achieved by Kumaraguru et al. (2007) and his colleagues, the research was carried out in a laboratory environment on students. Therefore, this study like so many others, suffers from the subject-expectancy effect. The subject-expectancy effect refers to a cognitive bias that occurs when a subject expects a given result and, therefore, unconsciously manipulates an experiment or reports the expected result, partly to avoid embarrassment (Ananpara et al., 2007:3).

As demonstrated by Kabay (2002), one way of holding the attention of users, inducing them to absorb the message and educating them more effectively, is through the use of the principles of social psychology. Kabay (2002) did this by addressing user group behaviour in order to render users more receptive to security policies and to bring about a positive change in their beliefs and attitudes in respect of IS security. The use of sanctions is strongly advocated (Kabay, 2002:35).

Furnell et al (2002:356) attempt to add context to security education by introducing security training software in terms of which scenarios are presented and users are expected to select the most appropriate control for the specific situation. This tool is useful as it provides an environment for users to simulate the use of countermeasures within an environment and it provides a practical method with which to enhance security. However, this approach, although a step in the right direction, does have limited applicability – it is geared towards small organisations and specific situations. In addition, the content may be best suited for individuals with a technical background, or else suited to a particular organisational culture – a small IT start-up company. No measurement of the effectiveness of the tool that was developed was carried out and, since this was a simulated experiment, it is unclear whether the same results would apply in the real world. Finally, Furnell et al. (2002) do not provide a theoretical foundation on which this research is based.

Further research in contextual-based training has been undertaken recently. There has been research in which social engineering techniques have been used against employees in their work environment. For example, Ferguson (2005:55) sent an official-looking internal email to a number of cadets to determine whether they would click on the bogus link it contained. His study found that 80% of the sample (512 participants) did click on the link, despite the fact that they had undergone four hours of information security awareness training (Ferguson, 2005:56). Ferguson merely used the results of this experiment as an awareness tool. Users must not only learn but they must be able to experience what is required in order to learn and, thereby, influence attitudes. The goal of awareness is to influence attitude. There are a number of gaps in this research work. Firstly the research looks at one type of security behaviour only. Secondly, Ferguson admits that training is not enough but, nevertheless, the effectiveness of training was not measured to ascertain whether or not it had made a difference. A control group was not used. Finally, this research shows that security professionals may expect too much from employees. For example, in this case the participants were expecting an email so it may have been unfair to expect them not to click on the link in the spoofed email that did appear legitimate. It may, for example, be too much to ask of our employees not to click on web links, as this is an integral part of the work environment and people click on them everyday.

Jagatic, Johnson, Jakobsson and Menczer, (2007:96) also used contextual phishing. They demonstrate that a large amount of information (accessible via social networking sites on the Internet) was easily obtainable and could effectively be used for phishing attacks. The researchers also wanted to measure the way in which social context information could influence the success of phishing attacks. They confronted challenges in carrying out human subject research experiments and had to adhere to federal standards in this respect. They also used a control group. The difference with this research is that these researchers tricked the users by spoofing emails that appeared as if they had come from friends in the users' social network. Seventy-two percent (out of 487 targeted students) of the students were taken in by the (harmless) phishing attack – this was a much higher percentage than had been anticipated (Jagatic et al., 2007:97). These researchers provide a baseline for successful phishing attacks and they also raise a number of interesting ethical questions in respect of researching social engineering attacks. They do, however, believe in the need for security awareness interventions to raise the awareness of end-users about phishing attacks but they are not sure how to measure the success of such awareness initiatives. This research does leave a few questions unanswered – what about other security-related behaviours (such as choosing a strong password) and would measuring other behaviours be as successful as it was with the phishing attacks? Also, the focus of this research is not to attempt to find a link between awareness training and the way in which end-users behave in terms of security. The researchers provided a stimulus, observed the resultant behaviour and reported on it – an effective research approach for their purposes.

Anandpara et al. (2007:1) show that, in their experiments, phishing tests (that determine whether users are able to identify phishing scams or not) are not in the least effective. Nevertheless, their findings did prove increased concern on the part of the participants (in respect of phishing attempts) but not the ability to identify phishing attempts after they had read phishing security awareness material. In addition, these researchers also showed that the various security indicators on emails that much of the security awareness material warns users to be on the alert for may easily be spoofed by phishers. They, therefore, imply that such forms of security awareness messages are ineffective. The tests that they carried out took the form of email screenshots that users had to study and identify as legitimate or not. The tests were administered both before and after the participants had been exposed to security awareness material on phishing. Anandpara et al. (2007:1) show that a high score is not necessarily an indication of an ability to identify phishing attempts. This research lacks real-world context and may skew the judgement of a test taker since static screens were presented to the user. Also, since the test takers are aware that they are being tested their level of suspicion may be heightened beyond what is normal as they will be expecting to be tested, although the researchers do maintain that their methodology took this into account.

Based on an assessment of students who had attended classroom training on phishing attacks, Robila and Ragucci (2006) demonstrate that such classroom training is effective. Their research focused on context-aware phishing, which may make users more vulnerable to phishing since these attacks contain user-context information as opposed to regular phishing (2006:237). For example, the group that participated in this survey was surprised that attacks could be launched by spoofed university or social networking sites (2006:241). Robila and Ragucci (2006) argue that a new education strategy is required to combat phishing threats and that this new strategy should combine regular IQ test phishing tests (request participants to identify whether an email is a phishing email) and classroom discussion training. They propose a way in which phishing education may be used as a tool – exposing students to the message and then teaching them how to identify phishing threats. They taught users what to look for and they then proceeded to show them legitimate and fraudulent emails in an attempt to determine whether they were able to identify fraudulent emails.

Thus researchers such as Anandapara et al. (2007) and Robila and Ragucci (2006) were able to demonstrate that it was possible for them to measure the effect of exposure to security awareness material although each research did produce different results. Thus hypothesis 1 of this research – end-user exposure to security awareness training has an effect on specific security behaviours – may be regarded as plausible. This research also considers another two hypotheses, hypothesis 2 – end-user exposure to security awareness training increases the internalisation of security knowledge – and hypothesis 3 – internalised security information is necessary in order for users to enact appropriate security behaviours.

Very recently there has been some work carried out which looks at ways in which training may become more effective and how to stimulate the interest of users in training material. In this respect the concept of "embedded training" and other novel methods will now be further explored.

Kumaraguru and his colleagues (2007b:907) also carried out research within a laboratory environment to determine the effectiveness of various security messages that warned users when they were doing something dangerous and the way in which individuals use this knowledge in various situations. They term this type of training "embedded training". Embedded training teaches users about phishing during their normal use of email. They found that common security notices warning about phishing attacks (typically sent out by commercial banks) were ineffective mainly because users are not able to understand why are they receiving these security notices and they are also not able to relate to the intangible problem being described (Kumaraguru et al., 2007:912). The researchers found that their embedded security messages were more effective than regular security messages in terms of the susceptibility of users to be duped by phishing attacks both before and after training interventions. They adhered to the principles of learning science in the design of their training interventions (Kumaraguru et al., 2007b:913). This research provides good insights into effective training methods. However, the study is affected by the subject-expectancy effect since a laboratory environment was used. Two methods were used for the embedded training and it was found that both these methods were more effective than regular security notices – this emphasises the importance of this type of training and of using learning principles in security awareness training.

Further research carried out on embedded training has demonstrated the effectiveness of this type of training. It has also proved that users retain more knowledge as a result of embedded training than they do after non-embedded training and that they were able to transfer this knowledge in that they were able to identify other types of phishing attacks more effectively. This was proved by testing the extent to which users retained the knowledge they had been taught after one week and their ability to use or "transfer" it to other types of phishing attacks (Kumaraguru et al., 2007c:70).

Whereas embedded training focuses on teaching users to spot phishing emails related research focused on teaching users to detect phishing websites. In the latter the researchers used a computer game that had been developed for users. As users played the game they learnt how to spot phishing attempts. It was found that users who had played the game were more proficient at identifying fraudulent (phishing) websites than those who had used the existing online training material as well as other material. The researchers are of the opinion that this is due to the content of the material and the interactive nature of the game (Sheng et al., 2007:88, 98).

2.4.1.3 Summary

As discussed in this section, previous research on information security awareness has been skewed towards awareness techniques. Although recent research has started examining the effectiveness of security awareness training the focus has been on phishing threats. This type of training has shown the effectiveness of classroom based training; email based training and web-based awareness material. The measuring of the effectiveness of overall security awareness, such as compliance with an acceptable usage policy within an organisation, and the examination of behavioural aspects has been largely neglected. In addition, very few theoretical models have been presented and used in order to explain and to test security behaviours.

2.4.2 Computer abuse and the insider threat

The 2007 CSI survey reports that insider abuse was perceived by the respondents as the most prevalent security problem within organisations.
For example, in January 2008, a man pleaded guilty to intentional damage to a "protected computer system". The man had planted a logic bomb on a hospital computer system. He had previously been hired by the hospital to develop a training program and had deployed the logic bomb on the system at that time. A few months after he had left the hospital the malicious software disabled the application he had developed – effectively rendering the hospital computer system unusable (FBI, 2008).

In another incident Ron Harris used his status as a computer laboratory technician for the Nevada Gaming Control Board between 1992 and 1995 to modify software that would rig slot machines to pay out jackpots in his favour (Schneier, 2003).

These stories are but two examples out of thousands of stories related to insider threat to organisations and computer abuse. Data theft also continues to be a major source of concern for organisations and it has impacted very severely on certain organisations. Some writers argue that it is impossible to protect organisations against insiders or "authorised abuse" (Dark Reading, 2007). The crux of the problem for organisations is that, even though they may secure their systems against hackers, database and system administrators are explicitly accorded full privileged access to the systems for administrative purposes. This, coupled with the administrator's technical knowledge and understanding of internal processes, makes computer abuse by insiders a serious risk to organisations. Therefore it has been argued historically that security awareness is important and that it may play a role in this context to combat these types of threats by

- alerting the colleagues of malicious employees to potential suspicious behaviour by explicitly stating what types of security behaviour are not allowed and how to report incidents
- acting as a deterrent to insiders if they are aware that they are being

monitored
- demonstrating due diligence on the part of the organisation in the event of disciplinary hearings being required

Much emphasis has been placed on the role of awareness in order to enhance vigilance on the part of employees in terms of security. Mitnick and Simon (2002:250) call for organisations to ensure ongoing security awareness to defend against, for example, social engineering attacks. The goal is to persuade employees to alter their behaviour and attitudes by motivating their employees to protect the organisational assets. Mitnick and Simon (2002:250) advocate the showing of a security film to render the security message more appealing to the audience. They also argue in favour of rewards and punishment to support the results of awareness training programmes (Mitnick & Simon, 2002:258) and, thereby, influence behaviour.

2.4.2.1 The role of deterrence in computer abuse

The emphasis of research on computer abuse and insider threats is on malicious employees and the focus on sanctions as will be explained further on. Merely making these types of employees aware of security policies for the sake of doing so becomes ineffective unless sanctions are imposed.

There are alternative countermeasures to be considered in this context. These countermeasures to avoid security breaches as proposed by Beatson (1991) include using psychological profiles, the surveillance of individuals and the application of the principle of least privileges. These are all implemented by means of the imposition of security policies and enhancing security awareness through security awareness training. Beatson argues that this would enable employers to recognise disgruntled employees before they could inflict much damage.

The majority of the studies on computer abuse by the users of IT systems have been based on the general deterrence theory (Lee & Lee, 2002:58). This theory maintains that computer abuse ceases when users are threatened. Detmar, Straub and Nance (1990:53) also made use of the general deterrence theory and found that, among other things, a high level of discernable investigative activities work well in preventing computer abuse. Their study also examined the way in which computer abuse incidents are discovered and how perpetrators are disciplined (Detmar et al., 1990:45).

Straub and Welke's (1998:445) work on the general deterrence theory (traditionally used to explain criminal behaviour) maintains that active and visible information security activity dissuades individuals from abusing computer resources since the perceived punishment, if caught, outweighs the risk. They further argue that actions on the part of managers may deter computer abuse, for example, information security awareness programmes. Their work explores whether managers are fully aware of those actions which have been shown to lead to lower system risks.

Straub's (1990:2) seminal work on the practicality of deterrence shows that: weekly hours dedicated to IT security and security in general, dissemination of IT security polices and guidelines, unambiguous communications to employees regarding the consequences of non-compliance and the use of IT security software were found to be the most effective IT security deterrents. He suggests that widely advertised efforts to detect non-complaint behaviour comprises a significant deterrent (Straub, 1990:19). He, therefore, recommends and promotes the use of sanctions in cases of known violations and maintains that such sanctions will have a deterrent effect on employees. This work is significant as it is a theory testing study which provides empirical evidence for the general deterrence theory.

In another study Straub, Carlson and Jones (1993) showed how users may be deterred from cheating on a programming assignment and suggests a number of steps that could be taken by managers in order to prevent computer abuse. These steps include encouraging the correct use of systems and stressing the fact that violations will lead to sanctions. This study also provides empirical support for the general deterrence theory.

2.4.2.2 Beyond deterrence as a countermeasure

Lee and Lee (2002:57) posed the question as to the reason why security policies, awareness activities and security systems are not effective as deterrents (despite the fact that they are have been widely regarded as such) and why computer abuse still persists. They suggest that it is because organisations have not applied the general deterrence theory correctly, and because the theory does not cover all the factors which lead to computer abuse (Lee & Lee, 2002:60). The research by Lee and Lee (2002) extends the computer abuse model (based on general deterrence) and explains the phenomenon in terms of social bonds and learning principles. They recommend that both technical and social solutions should be implemented in order to solve the problem of computer abuse. Their model is based on the assumption that the behaviour of an individual is determined by behavioural intent. These intentions are, in turn, affected by attitudes and social theories (2002:60) which may be shown to affect computer abuse decisions. For example, it has been shown that there is a strong positive correlation between a friend's involvement in computer abuse and the probability of computer abuse. Thus security awareness may be seen as another tool with which to limit computer abuse.

Thus, since most of the computer abuse studies are seen through the lens of the general deterrence theory security awareness activities are perceived as a preventative measure. Studies on computer abuse have focused on “insiders” with malicious intent with the threat of sanctions as the most effective deterrent and awareness initiatives used a medium to convey the message. Thus computer abuse research is focused on negative behaviour and does not demonstrate the effect of awareness training on behaviour.

Since it is widely accepted that the most significant threat to the security of an organisation is its staff (Gaunt, 2000:152) more contemporary researchers have focused on other relevant factors such as the importance of staff attitude (and, in turn, a demonstration of commitment on the part of key leaders within the organisation). In addition, other factors such as perceived security threat and the perceived self-capability actually to affect the necessary behaviours are also seen as factors which affect security behaviour (Woon, 2005:367). This type of research will be examined further in the following section on behavioural information security.

2.4.3 Behavioural information security

The importance of inducing individuals to act correctly has always been implied in previous research work. However, recently there has been a more explicit focus on the behavioural aspects of security. Behavioural information security is a branch of information security research which examines those factors which motivate security related behaviours in computer users. Recent work in behavioural information security has also demonstrated the way in which employee job attitude relate to information security behaviours (Stanton et al., 2003); categories of information security behaviours (Stanton, et al., 2005); factors influencing information security behaviours (Leach, 2003); the way in which attitudes and intentions constitute significant factors in explaining the reasons why certain employees do not comply with information security policies (Pahnila et al., 2007) and how a design theory for a security awareness programme was effective and was shown to achieve positive results, change user attitudes and make users more conscious of their behaviour. More practical studies of this nature are called for (Puhakainen, 2006:106, 114, 139).

Kajava and Siponen (1997:113) adopt a human-centric perspective when they state that the awareness approach must understand and respect human factors in order to obtain buy-in from employees into the security awareness initiatives. This focus on the human element is also supported by Perry (1985:92). An example of this approach entails ensuring that the security requirements do not interrupt/impact on employees too heavily (Kajava & Siponen, 1997:111). This view is supported by Parker (1998) who calls for security to be made part of an employee’s job performance, thus eliminating conflicts between security and job requirements.

2.4.3.1 The influence of social psychology

Certain researchers have also linked their research to the field of social psychology. Siponen (2000a:33–34) argues for awareness programmes to be based on behavioural theories. Security practitioners should persuade users of the reasons why it is important to follow guidelines by means of a framework which targets the motivations and attitudes of end-users. This would ensure that they internalise and comply with the policies. Accordingly he proposes a framework for persuasive approaches grounded in ethics and morals (Siponen, 2000a:37–38). Siponen's framework (2000a) is based on a number of theories including the theory of reasoned action and the theory of planned behaviour.

Aytes and Connolly (2003) propose a theoretical model based on social psychology to attempt to explain the reasons why employees engage in behaviour that contravenes information security policies. The model proposed is based on the user's perception of risk and the choices made based on that perception. A user's knowledge (such as the consequences of certain behaviours) is informed by various resources within his/her environment (for example, colleagues, systems, policies, training). It follows that a user's perception determines the specific behavioural choices which drives actual behaviour (for example, whether to abide by a policy or not). Such behaviour then has an outcome which feeds back into the user's knowledge and perceptions. Briefly the user's behaviour is affected by his/her perceptions of the personal and organisational trade-off of the behaviour (Aytes & Connolly, 2003:2028–2029). Their model is based on previous work in respect of human perception and reactions to risk.

Thomson and von Solms (1998) also drew on principles from social psychology and called for these principles to be deployed to improve practical effectiveness of IS security awareness. Their goal was to increase the understanding of user attitude.

Kruger and Kearney (2005) developed a prototype for measuring the effectiveness of a security awareness program that was delivered within a global organisation. The model that they developed was based on techniques from the field of social psychology which maintain that individuals respond in a certain way because of three factors, namely, affect (emotions about something), behaviour (intention to act in a certain manner) and cognition (belief about an object). Kruger and Kearney (2005) then translated these factors into a model that could be measured, that is, what a person knows (knowledge), how the person feels about a topic (attitude) and what the person does (behaviour). These three dimensions are measured in order to determine the effectiveness of the awareness programme. Information was gathered using questionnaires (including assessing intended behaviour) although they do suggest using system data at a later stage.

Thus the actual behaviours of the employees were not measured in order to determine whether there had been a difference effected in these behaviours. Kruger et al. (2006) also recommend that system data be gathered to supplement employee surveyed data and propose a basic list of source data from systems that could be used and also the purpose for which this source data could be used.

The work by Kruger et al. (2006) also makes use of the value–focused procedures proposed by Keeney (1996:537). These procedures are used to illustrate cause-effect relationships, and show how the decisions taken by managers of an organisation were motivated by the values of those managers. This methodology was then used by the organisation in question to identify the areas of security on which to focus (Kruger et al, 2006). This is a meaningful piece of research and there is merit in examining this value-focused approach and security objectives more closely in the future.

Pahnila et al. (2007) proposes a theoretical model that is used firstly to elucidate those factors which contribute to employee compliance with security policies and, thereafter, ways in which this compliance may be enhanced. This model is then validated empirically. Pahnila et al. (2007) maintain that one of the key factors in assessing whether users comply with security policies is determined by the strength of the users' intention to do so. They hypothesise that this, in turn, is determined by sanctions. They demonstrate the complexity of security behaviour by postulating that compliance with policy, in fact, comprises the intentions and attitudes of employees (which are, in turn, determined by various factors). They, therefore, recommend that promoting positive social pressure on employees with respect to compliance with security policies (for example, by all levels of management and also peers within organisations) enhances actual security compliance. This should be done by stating explicitly what is required and the correct behaviour should be demonstrated by senior management. This is in line with research carried out by Leach (2003). One of the factors that influences user security behaviour is what is conveyed to the users. In most organisations this communication takes the form of security policies and security awareness initiatives (Leach, 2003:686). Another influencing factor in this regard is what the employees perceive to be happening around around them. Employees are strongly influenced by their peers and by the messages which are sent out by the organisation – whether internally or externally. If employees perceive inconsistencies and contradictions between the message and the actual behaviour within the organisation these perceptions will ultimately influence their behaviour (Leach, 2003:687).

2.4.3.2 Security Culture

Standards bodies and researchers have also highlighted the importance of security culture and its relationship to security awareness. In order for appropriate behaviour to take effect a security culture needs to be in place within the organisation. It, therefore, follows that, in order for such a culture to be in place, it is essential to educate the employees (Van Niekerk & von Solms, 2004). Martins and Eloff (2002:206) present a model of security culture and a tool with which to measure it that may be utilised to improve the security culture within an organisation (2002). The model focuses on three levels within an organisation – organisational, group and individual. These researchers believe that human behaviour needs to be taken into account in addressing cultural security issues. This may be achieved by initially ensuring that each employee is informed through security awareness training so that they are aware of what is expected of them. Thereafter the group and organisational levels are dealt with to influence the culture one level at a time. Other factors such as the values and beliefs of individuals may also affect end-user behaviour. Thus, even though an employee may have fully understood the policy he/she may not act as required if there is a conflict with his/her belief system (Schlienger & Teufel, 2003).

Schlienger and Teufel's (2002) model for information security culture explains the way in which the cultural theory may help to enhance the overall security within an organisation. The most important aspect of security culture is the requisite standard of behaviour on the part of managers, the training of employees and rewards for good behaviour. This view is echoed by Gaunt (2000:151, 157) who believes that information security awareness initiatives, while important, do not guarantee that staff will manifest the appropriate security behaviours. With reference to the healthcare community he argues that a security culture needs to be entrenched for security to be effective. This requires, inter alia, strong commitment on the part of senior management, and clear lines of accountability and responsibility (Gaunt, 2000:157; Kajava & Siponen, 1997; Mitnick & Simon, 2002:252).

Vroom and von Solms (2004:191–192, 194, 197) have also recognised the importance of human behaviour in the security chain but from an auditing perspective. They put forward the argument that, although auditors express an opinion on the financial and IT setup of an organisation employee behaviour – a key aspect of information security - is not measured. They claim further that the reason that end-user behaviour is often neglected is because it is so very difficult to measure and that such measurements will inevitably be flawed. The auditing of end-user behaviour is compared to the carrying out of employee performance appraisals and the resultant flaws associated with this activity – reliability and validity. They believe that there are too many factors that may interfere with the accurate "auditing" of the employee. They, therefore, propose an alternative approach for the auditing of behaviour and suggest that it might be preferable to attempt to change organisational culture one level at a time and, thereby, influence end-user behaviour.

The work of Vroom and von Solms has significant implications for this study.

The fact that this study demonstrates that it is possible to measure behaviours both contradicts and adds a new dimension to the notion put forward by Vroom and von Solms. In addition, the techniques used and the lessons learned will form the groundwork for further research work.

According to Gaunt's studies (2000:152–153) there are a number of obstacles that need to be overcome to ensure that security measures are effective and a culture of security instilled. These obstacles include the following:

- Users may have become accustomed to using the computer systems in an insecure way and this would make it more difficult to induce them to change their behaviour. The enforcing of stronger security measures may, in reality, cause greater reluctance on the part of employees to change their behaviour. In addition employees may view security measures as impractical and a hindrance to their work.
- Being unaware of exactly what is required of them may also bring about a reluctance to embrace security.
- Inconsistent application of policies among or within organisations may lead to frustration on the part of employees and this may, in turn, undermine the effectiveness of the policies.

Gaunt's (2000) research provides insight into the obstacles confronted by practitioners although his work does lack a theoretical basis. It does, however, indicate the nature of the problem.

2.4.3.3 Ethical foundations

There has also been research work carried out that highlights the role of ethics in terms of security behaviour. Banrerjee, Cronan, Jones (1998:31) concur with Leach's stand about the fact that correct behaviour must be demonstrated by leaders within the organisation, but they view behaviours through an ethical lens. They identify situational circumstances which influences the ethical intentions of users when users are faced with ethical dilemmas. After carrying out an empirical study to test their theory they concluded that the intention on the part of employees whether to act ethically in the workplace is influenced by the way in which they perceive their organisational environment and conditions, and their moral obligation to behaving correctly. These researchers propose that the solution would be to ensure that the ethical requirements of the organisation are made clear to employees and that there are strong deterrents to incorrect security behaviour in place (Banrerjee et al., 1998:49). Thus the significance of security awareness in conveying the security message is critical. Nevertheless, individual characteristics and beliefs also play an important role in behaviour and must be taken into account. Similarly, the work by Forcht et al. (1988) proposes the use of information security awareness techniques to create, promote and maintain a strong ethical foundation within an organisation and, thereby, promote information security issues. They also emphasise the importance of attitudes and the role of right and wrong within organisations. They explore ethical problems within IT environments.

Instead of explicit security awareness training certain writers argue that the focus should rather be on ethical education in order to improve the security behaviour of employees. Ethical principles would then form the foundation of correct and incorrect behaviour. (Siponen, 2000b; Kluge, 1998). In this respect linkages between specific security acts and ethical principles would be forged and demonstrated and a climate of justifying security behaviour to be either morally acceptable or not would be brought about (Siponen, 2000b). Kluge proposes the need for a code of ethics to be used to enlighten and guide personnel on security matters, and, thereby, encourage security behaviour - specifically in terms of the medical environment in which the need to protect patient information is critical.

While conveying the security awareness message is considered to be important it is also critical to ensure that it is possible to measure the effectiveness of the security awareness initiatives (Kruger et al., 2006). As mentioned, however, more research is required on the link between security awareness initiatives and the outcomes of such initiatives – in other words the behaviour of employees within organisations as a result of these initiatives. Schultz (2004:1) calls for further research on the benefits of information security awareness and training. Srikwan and Jakobsson (2007:2) agree with this call and maintain that sufficient attention has not been paid to this aspect. They add that the main challenge is the fact that the problem is multidimensional – a combination of social and technical problems.

It is necessary to ensure that the information security awareness initiatives are adequate, appropriate and effective. To this end Kruger et al. (2006) propose a framework for measuring the effectiveness of awareness initiatives while at the same time they suggest a way to determine those areas that need to be evaluated. Evaluation of the effectiveness of the security awareness initiatives should also identify possible areas of improvement (Hansche et al, 2004:69; Schlienger & Teufel, 2005).

2.4.3.4 Extending and building on the work of Stanton et al.

This research adopts the model proposed by Stanton et al (2005) in order to draw conclusions about whether awareness training does have an effect on specific behavioural categories. This model states that all security behaviour may be plotted on a behavioural continuum. On one level behaviour is categorised based on the intentions of the user – from malicious to neutral to benevolent behaviour. On another level behaviour may be categorised based on the level of expertise of the user ranging from novice to expert and something in between the two. This approach produces a two-factor taxonomy of user security behaviours which yields six broad behavioural categories as illustrated in figure 3 below. This research focuses on those behaviours that require low technical expertise and it maps those behaviours against this model.

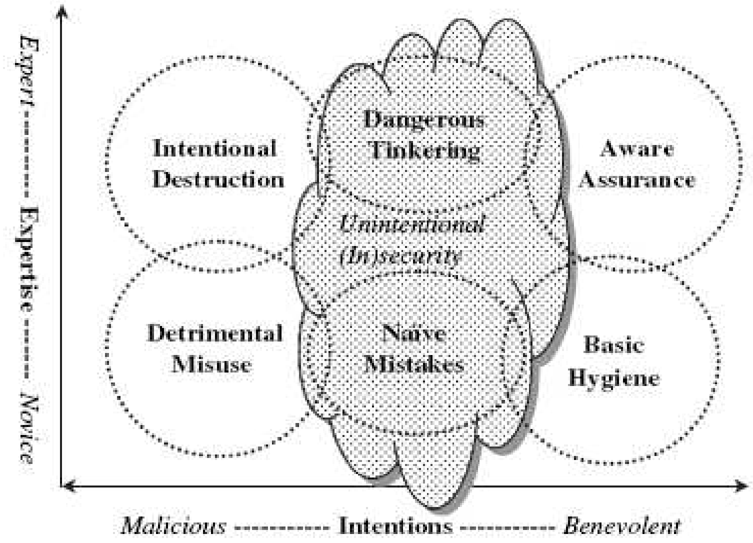

Expert -------- Expertise -------- Novice
Intentional Destruction
Dangerous Tinkering
Aware Assurance
Unintentional (In)security
Detrimental Misuse
Naïve Mistakes
Basic Hygiene
Malicious ----------- Intentions ----------- Benevolent

Figure 3. Two-factor taxonomy of end-user security behaviours (Adopted from Stanton et al. 2005).

The goal of this security awareness research is to move the intentions of employees towards the right-hand side of the chart. In this way Stanton et al. (2005:132) provide a practical framework for categorising information security behaviours. This model now lays a foundation for the measurement of security behaviours. This research measures those behaviours which require low levels of expertise i.e. Detrimental Misuse, Naïve Mistakes and Basic Hygiene.

An illustrative example of the above taxonomy is presented in table 2 below:

Table 2: Examples of behaviours that require low levels of expertise.

Behaviour	*Intent*	*Expertise*
Employee sends pornographic material to colleagues.	*Malicious*	*Low*
Employee shares password with his wife.	*Neutral*	*Low*
Employee chooses a strong password.	*Benevolent*	*Low*

This research report measures end-user security behaviours in a formal manner in order to determine whether the awareness training to which individuals were exposed will make a difference to their future behaviour. Stanton et al. (2005:124, 131) used simple correlation to show that good password practices (changing passwords frequently and choosing strong passwords) were associated with training and awareness, knowledge on the part of employees that they were being monitored and organisational benefits as perceived by the employees. However a positive correlation does not necessarily mean that these good password practices were the result of training and awareness.

Interestingly Stanton et al. (2005) did not find any correlation with another type of naïve security behaviour – that of sharing one's password. They concluded that there is no evidence that password sharing behaviour is associated with training, awareness, organisational rewards and the knowledge of being monitored (Stanton et al., 2005).

Additional research is needed in this area and is called for explicitly by Stanton et al. (2005). Different techniques are used in this research which yield different results to those obtained by Stanton et al. (2005). For example, Stanton et al. used surveys to gather their data whereas this research used direct observation. This research report contributes to the existing information security awareness literature and extends it. In other words, a portion of the model presented by Stanton et al. will be used to draw conclusions about whether awareness training had an effect on specific behavioural categories.

2.5 SUMMARY

It was discussed in this chapter that there is a dearth of in-depth information security awareness research and that behavioural concepts are not properly taken into account in security awareness programmes. The information security awareness literature falls into one of three categories. Most of the literature is related to the importance and the techniques of security awareness. Then there is research on computer abuse and the threat of insider abuse. Finally, Behavioural Information Security is a relatively new field that examines the motivations behind security behaviours. Information security awareness research relating to: the influence of social psychology on security behaviour; the role of security culture and ethical considerations are grouped under behavioural information security.

There is a lack of research on Behavioural Information Security and theoretical models which explain the way in which awareness training affects behaviour. Specifically, there is a shortage of research demonstrating the practical effectiveness of Information Security awareness training. Where studies do exist they focus mainly on the effectiveness of anti-phishing training. Secondly, aside from the research by Jagatic et al. (1997), no other studies were found that used direct observation in order to measure security behaviour. This study builds on existing behavioural information security research, namely, the model proposed by Stanton et al (2005) in order to draw conclusions about whether awareness training has an effect on specific behavioural categories. A theoretical model, based on an organisational learning model, explains the way in which organisational learning takes place. This model shows that both explicit knowledge and implicit knowledge are needed.

CHAPTER 3 : MEASURING SECURITY BEHAVIOUR

> You should write the Methods chapter as a reasoned argument toward the conclusion that the questions can be answered (or hypotheses confirmed) … by analyzing data that can be collected from a viable sample.
>
> Jens Mende (2006)

3.1 INTRODUCTION

The previous chapter highlighted the shortcomings and limitations of the existing security awareness research. The purpose of this chapter is to present a detailed research strategy – in terms of sampling, data collection and data analysis – for achieving the objectives which were introduced in Chapter 1. The goal of this research perhaps merits being restated – to determine the effect of exposure to security awareness training on end-user behaviour. Three hypotheses were tested.

The first hypothesis comprises a composite construct made up of three sub-hypotheses. This hypothesis states that end-user exposure to security awareness training has an effect on three specific security behaviours – End-user exposure to security awareness training on appropriate information handling improves the secure handling of information; End-user exposure to security awareness training on acceptable usage of e-mail and Internet facilities diminishes Internet and e-mail abuse on the part of end-users and, End-user exposure to security awareness training on password management best practices improves the secure handling of passwords by end-users.

The second hypothesis proposes that end-user exposure to security awareness training increases the internalisation of security knowledge while the third hypothesis proposes that internalised security information is necessary in order for users to enact appropriate security behaviours.

The research approaches adopted in this study are presented in table 3 below. The previous two chapters used conceptual analysis in order to identify the existing information security awareness landscape, shortcomings in the existing material and possible areas of improvement. In terms of conceptual analysis the presence of an existing concept is examined, considered and categorised (Methods of Conceptual Analysis, 2008) including explaining the implications and inconsistencies of the concept (Welman & Kruger, 2001:24).

Table 3: Research methods used (Adopted from Puhakainen, 2007)

Research Step	*Chapters*	*Research Approach/Strategy*
Introduction and literature survey	*1 & 2*	*Conceptual analysis*
Research methods and results	*3*	*Action research and case study*

This research also used action research as the preferred research method. In terms of action research the problem is identified, a plan of action with which to address the problem is developed and implemented, and the data is collected and evaluated. The actual implications of the findings are then discussed (Baskerville, 1999). Action research is suitable for examining information systems methods in a practical setting and studying the appropriateness of the research in real-life (Baskerville & Wood-Harper, 1996).

Puhakainen maintains that action research is an empirical method and a form of research in terms of which the researcher becomes involved in solving the actual, practical problems experienced by an organisation (Puhakainen, 2006:11).

It therefore follows that a case study would be chosen as the appropriate strategy for this research as this approach corresponds with action research in the sense that the question under examination arises in the case study in question. The case study approach was also beneficial because this research was coupled with the existing information security awareness activities within the organisation.

Therefore the coupling of the planned security awareness activities with this research provided a dual benefit – it provided data for the research while it also provided security awareness training to employees on the Acceptable Usage Policy (AUP) of the organisation. This research also measures the effectiveness of such training in the organisation. In this sense the organisation in question is able to make a decision on whether the approach to awareness training was successful or not and whether the organisation should continue with the same strategy in the future or adopt a different approach. The researcher of this report played an active role by executing the security awareness activities at the organisation as well as gathering the data that is the subject of this report.

The organisation that was the subject of the case study is a South-African based company that operates in various countries. The headquarters of the organisation are in South Africa and it has a staff complement of 5 726 employees. Although the approval of the organisation was obtained prior to carrying out the research within the organisation the company will remain anonymous in this report. As with all organisations, the organisation in question, which henceforth will be termed Topaz CC, was concerned about security within the organisation. This is especially true in terms of the protection of customer information that the organisation stores and processes. The protection of such information (as in the case of other information) is mandated by South African law.

Topaz CC has fairly recently both approved and promulgated a number of information security policies. One of the most important of these policies is the AUP (Acceptable Usage Policy). The AUP (see Appendix A) comprises a single document that covers all end-user responsibilities including all employees or third-parties accessing Topaz CC's network (for example, consultants and suppliers). This organisation, in common with many others, has experienced a number of incidents and blatant violations of its AUP by employees. Therefore the first step was to ensure that users were aware of their security responsibilities and the actions that they should take in order to become more secure. In the past security awareness activities at Topaz CC had been scanty and haphazard and had consisted of occasional emails sent to all employees on certain topics such as clean desk policy, correct email usage and emails regarding the threat of viruses and phishing scams. Emails had been used as they were considered the most efficient method of communicating with all users. Consequently, email was used for all end-user communication and the end-users had been bombarded by emails on a daily basis. The existing AUP had been completed in 2006 and included a user friendly security guideline booklet. The AUP consists of various sections on end-user responsibilities such as software usage, email usage and mobile computing. For each section the guidelines booklet illustrates a scenario using cartoon strips in order to render the message more acceptable to the users. The booklet was distributed to end-users during 2006. During 2007 various security emails were sent to end-users on specific topics contained within the AUP every two months.

3.2 RESEARCH STRATEGY

3.2.1 Overview

The following diagram depicts the sequence of activities which were followed during this research. This information is presented in order to provide the reader with a perspective on the nature of the research. Thereafter, a more detailed discussion on the techniques followed will be presented.

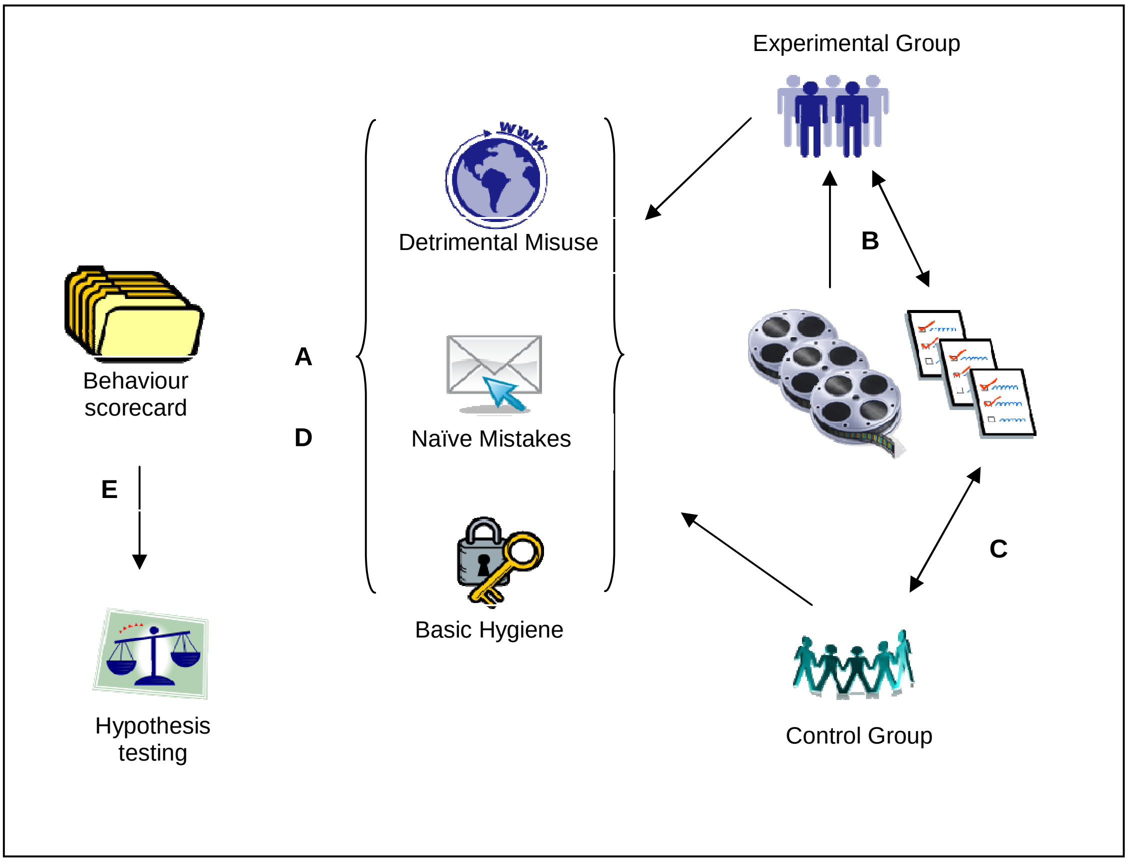


Figure 2. High-level overview of research approach

Initially, three security behaviours on the part of the control and the experimental group members were measured. These behaviours were categorised as Detrimental Misuse, Naïve Mistakes and Basic Hygiene. The measurements were entered on the security behaviour scorecards of each of the control group and experimental group members (A). Thereafter the members of the experimental group were exposed to the security awareness training film (delivered in three separate parts) and the accompanying security test (B). The control group members were not exposed to the training but were required merely to complete the security test (C).

The security behaviours of the control and the experimental group members were again measured, collated and entered on the security behaviour scorecards (D). Thereafter the security behaviour scorecards were used as input to test the validity of the hypotheses proposed in this report by using the statistical techniques described in this chapter (E).

3.2.2 Statistical techniques employed

In most cases non-parametric statistical techniques have been used. The reason for this is the different sample sizes which were obtained from the control and the experimental groups. In addition, some of the experimental group sample sizes were much smaller than the control group sizes. There was thus some concern about the normality of the data. The reason for this difference in the sample sizes is to be found in the fact that the control group members merely had to complete the necessary security tests whereas the experimental groups had to watch a security film and then complete the security test. Thus, the experimental group members may have found the process too onerous. In cases where parametric tests have been used the data meets the general assumptions for parametric tests, namely, the samples are random and the observations are independent (Pallant, 2001:255,256).

3.2.3 Security behaviour measurement strategy

In order to test the three sub-hypotheses for hypothesis one the extent to which the security behaviour complies with the AUP must be measured since the AUP specifies what comprises acceptable and unacceptable security behaviour. The AUP for Topaz CC is a relatively lengthy document for a layperson to read and it consists of nine security sections or topics. Within these nine security topics multiple policy statements will apply depending on the specific topic. For example, the section on email usage consists of directives on the primary use of email, automatic forwarding of email, the use of webmail accounts, prohibited email activities etc.

Accordingly, there are many potential security policy statements that could be measured for compliance. However, a subset of these policy statements only was measured. The decision regarding the measurement of those policies with which end-users comply is based on Stanton's taxonomy of security behaviours. The strategy of this research is to use the taxonomy of behaviours developed by Stanton et al. (2005) as a foundation for classifying the behaviours to be measured. The choice was made to measure those behaviours that require a low level of technical expertise. These behaviours must, of course, also appear in Topaz CC's organisational policy so that it is possible to measure compliance with the organisation's security policy.

Table 4 below maps the actual AUP statements to the hypothesis to be tested and explains the rationale for choosing a particular policy statement to be measured and why each particular policy statement reflects the hypothesis in question. This demonstrates that measuring the hypotheses also measures compliance to portions of the organisation's AUP. If the behaviour can be mapped to a policy then we can make conclusions about the security of an organisation (based on compliance to the policy). This method is something that security practitioners could find useful for their organisations.

Table 4: AUP sections to be measured mapped to research hypotheses

Hypothesis to be tested	*Intent*	*Skill*	*Policy statement in Acceptable Usage Policy*	*Rationale*
H1a: End-user exposure to security awareness training on appropriate information handling improves secure handling of information. Behaviour category: Naïve mistakes	Neutral	Low	*"Your user ID and password are the key defences for the organisation's equipment, systems and information. In order to protect these, you are expected… not to share your password with anyone, including IT support staff…"*	It is argued that your password is one of the most sensitive pieces of data available since is it the key to your information and must be handled with great care. It does not require high technical expertise to share your password with other individuals but it does require users to be cautious. Intentionality rating is considered neutral if the password is given away carelessly.
H1b: End-user exposure to security awareness training on acceptable usage of e-mail and Internet facilities diminishes Internet and e-mail abuse on the part of end-users. Behaviour category: Detrimental misuse	Negative	*Low*	*"Occasional personal use of the Internet is permitted at the discretion of your manager… Follow the corporate principles regarding resource usage and exercise good judgement when using the Internet"*	Abuse of Internet facilities is considered behaviour with a malicious intent since organisational resources are being abused. The organisation is also placed at risk if users download spyware (deliberately or inadvertently) when using Internet facilities. Indirectly, the organisation is affected since the user spends more time on the Internet than working. It, therefore, follows that the greater the abuse of Internet facilities the more detrimental this is to the organisation.
H1c: End-user exposure to security awareness training on password management best practices improves secure handling of passwords by end-users. Behaviour category:Basic hygiene	Positive	Low	*"..you are expected…to use well chosen passwords... ensure that consists of mixed case, numerical characters and special characters and avoid the use of personal information and dictionary words in the password."*	The focus of this policy is on choosing passwords that are difficult for attackers to guess yet easy for the owners to remember. This is considered positive or beneficial intention as users are consciously choosing strong passwords and thereby ensuring their user account is more secure. Technical expertise is not required in order to choose a strong password.

These policy statements are corroborated by studies carried out by Stanton & Stam (2006:313-314) in which they requested a group of security experts to categorise a list of 93 behaviours in terms of intentionality (positive, negative or neutral), and in terms of the expertise needed to execute that behaviour (lower, middle and high). Discussions with a security expert in South Africa also confirmed that measuring the policy statements above would be appropriate in terms of testing the corresponding hypothesis. So, for example, in terms of Hypothesis 1a, in testing the impact of training on the secure handling of information the policy statement prohibiting sharing of passwords was tested. Secondly, in terms of Hypothesis 1b in testing the impact of Internet usage training on end-users the policy statement on the correct and incorrect use of the Internet was tested. Likewise, in terms of hypothesis 1c, in testing the impact of training on the usage of passwords by end-users the policy statement requiring a specific composition of passwords was tested.

3.2.3.1 Sampling

Both control and experimental groups were used for the research design. The reason for this is that the use of a control group is considered the most practical way in which to control nuisance variables. Therefore, the behavioural measurements described in this chapter were measured for both the control and the experimental group members. The candidates for both were employees of the organisation. Thus, the population (*N*) was 5,726. The organisation consists of a number of distinct strata based on the organisational departments each of different sizes, cultures, and priorities. In addition, as a result of the nature of the organisation, there are a large number of contractors working in the organisation. Different cultures exist, for example; consider the differences between field engineers as opposed to call centre personnel. The nature of the research demanded that the sample size be as large as possible.

The criterion for choosing the groups was that all candidate members had to have Internet access. This was important since two of the behavioural measurements for testing hypotheses 1a and 1b (Naïve Mistakes and Detrimental Misuse) measure end-user susceptibility to a phishing mail and Internet browse times. Thus, a list of all end-users who had Internet access was generated. This amounted to 8 600 entries and included system accounts as well as end-user accounts.

Many targets were removed from the sample as they were considered invalid. For example, there were no browse times available for the end-user, and certain entries were system accounts or IP addresses. Some employees who had joined the organisation very recently as part of a company acquisition were also excluded. Finally, executive accounts and persons associated with executives in some way were removed as the researcher wanted to ensure that the end-users were not interfered with in any way during the fieldwork. The final, viable sample size (*n*) totalled 2,144. Thereafter the list of end-users was divided into control and experimental groups as follows. A random number (between 1 and 10000) was generated and assigned to each end-user in the sample. The *RANDBETWEEN* Microsoft Excel function was used to generate these random numbers. The list of end-user was then sorted by their assigned random number from smallest to largest. The first half of the list (1,072) was allocated to the control group and the second 1,072 entries were allocated to the experimental group.

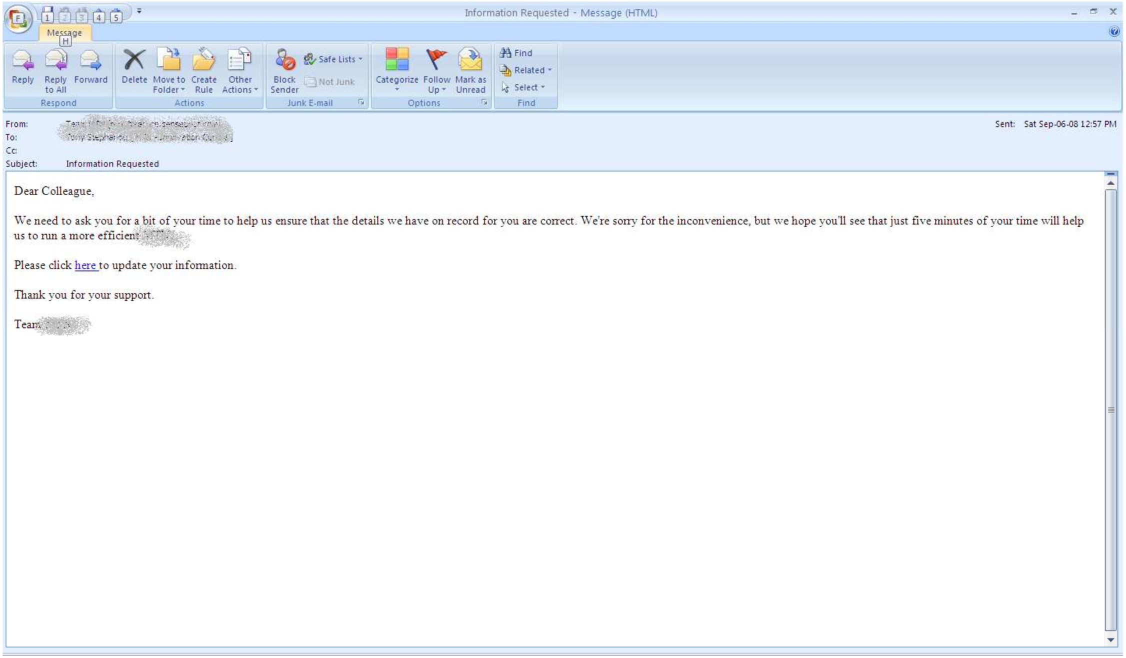
3.2.3.2 Data collection

Once the policy statements to be measured had been agreed upon the next step was to select the most appropriate mechanism with which to measure these policy statements. Table 5 below illustrates the variables required in order to measure these policy statements.

Table 5: Hypothesis 1 mapped to variables

Hypothesis Description	*Indep. variable*	*Dependent Variable Measurement*	*Analysis*	*Dependent Variable Score Calculation*
H1a: Naive Mistakes (Neutral Intent): End-user exposure to security awareness training on appropriate information handling improves secure handling of information.	Binary: Viewed security awareness film (Y or N)	A binary variable was used. The mechanism employed comprised a (harmless) doubtful email sent from a fictitious email address to the sample, but purporting to come from Topaz CC. The email requested users to update their information on file by clicking on the link provided.	Chi-Square	Should end-users click on the link in the email a value of ("Y") is assigned to the person's user ID. Otherwise a value of ("N") is assigned to the person's User ID.
H1b: Detrimental Misuse (Malicious Intent): End-user exposure to security awareness training on acceptable usage of e-mail and Internet facilities diminishes Internet and e-mail abuse on part of end-users.	Binary: Viewed security awareness film (Y or N) – Binary	A continuous variable was used. Internet browse time activity (in minutes) over a two week period was measured.	Independent-samples t test	Raw browse times in minutes were used. These were obtained from the corporate web monitoring tool – SurfControl.
H1c: Basic hygiene (Beneficial Intent): End-user exposure to security awareness training on password management best practices improves secure handling of passwords by end-users.	Binary: Viewed security awareness film (Y or N) - Binary	A binary variable was used. Password hashes for sample users were extracted and run through a freely available password cracker in an attempt to identify weak passwords.	Chi-Square	Users with passwords that could be cracked, received a value of "Y" otherwise a value of "N" was assigned.

In terms of the Naïve Mistakes behaviour measurement (H1a) an email was devised to be sent to both the control and the experimental group members. The purpose was to determine whether end-users would be duped by an email that looked as if it had come from Topaz CC. The email requested the users to update their details by clicking on a link provided. In actual phishing cases once an end-user is taken in by an email and clicks on the link they are likely to enter their credentials into the fake website to which they have been directed. In this way criminals are able to "phish" passwords. Thus if a user clicks on the link provided in this exercise it is assumed he/she would provide his/her credentials if prompted to do so. Care was taken to ensure that the email did not look completely authentic as it was felt that this would have been unfair to end-users. The email contained a number of clues that should have raised the alarm for vigilant end-users. For example, although the name of the sender appears to be legitimate ("Team TOPAZ CC") the actual email address has another domain name. On the other hand, care was taken not to make the email too obvious.



From: [redacted]
To: [redacted]
Cc:
Subject: Information Requested

Sent: Sat Sep-06-08 12:57 PM

Dear Colleague,

We need to ask you for a bit of your time to help us ensure that the details we have on record for you are correct. We're sorry for the inconvenience, but we hope you'll see that just five minutes of your time will help us to run a more efficient [redacted]

Please click here to update your information.

Thank you for your support.

Team [redacted]

Figure 3: Actual email that respondents received.

The system was designed in such a way that once users had clicked on a link their user ID was registered on a central database located on the Internet. The end-users were not directed to a website nor were they prompted for their credentials.

In terms of the Detrimental Misuse behaviour measurement (H1b) the design comprised the use of standard reports from Topaz CC's corporate web monitoring tool – SurfControl. Reports were generated for both the control and the experimental group members. These reports indicated their browse times in minutes over a two week period.

In terms of Basic Hygiene behaviour measurement (H1c) the design required that the passwords used by both the control and the experimental group members were tested for strength. The design involved the use a freely available password cracker termed *John the Ripper* (also known as John). John contains various options for cracking passwords, but, in the end, it was decided to use the wordlist option with word mangling enabled. This meant that John would compare user passwords to words and phrases found in a wordlist. In this case a 42MB wordlist containing the most common and also not so common passwords and passphrases was used. The word mangling feature was also used. This creates numerous variations of each password/passphrase found in the wordlist. Therefore, running John in this mode generates a vast number of possible passwords and passphrases which are compared with the user passwords which have been extracted. In this way common and weak passwords are easily and quickly identified.

The three security behaviours described above were designed to be measured twice: once prior to security awareness training and once subsequent to security awareness training. Obviously the control group did not undergo security awareness training. This process is depicted in table 6 below.

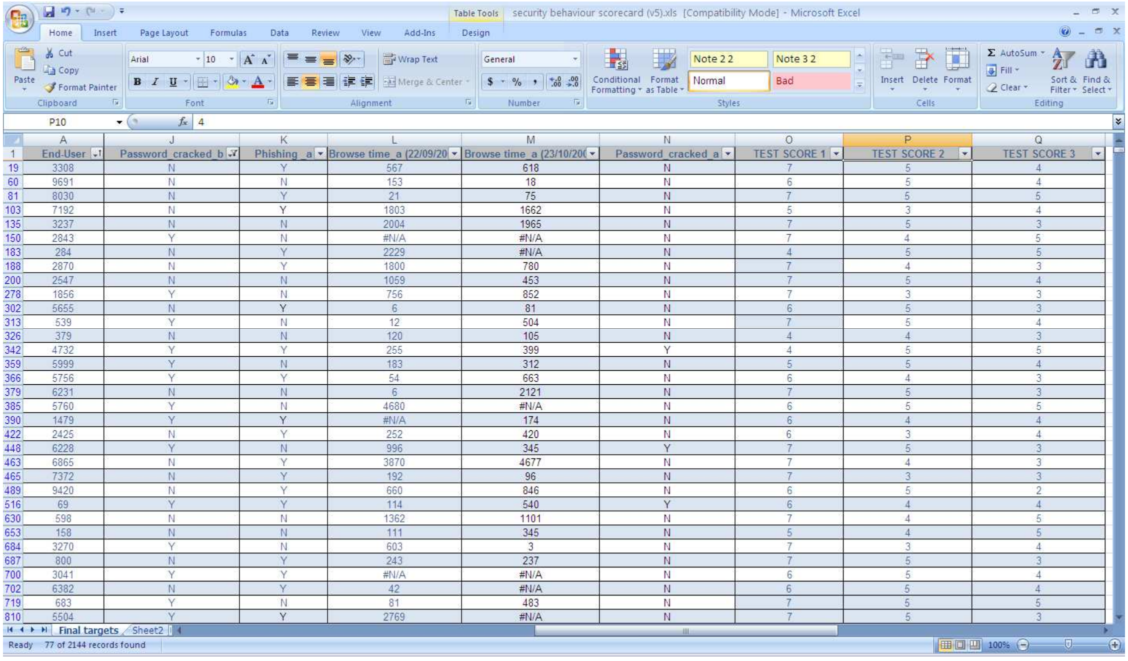
Table 6: Research design

Group	Measure 3 Security Behaviour Indicators	Provide Security Awareness Training	Measure 3 Security Behaviour Indicators
Control Group	✓		✓
Experimental Group	✓	✓	✓

Once all these variables had been successfully collected a security behaviour scorecard was created for each control and each experimental group member. A sample score card is depicted in figure 4 below.

3.2.3.3 Data analysis

Figure 3 below is a screenshot of a populated security behaviour scorecard once the data described above has been collected.



	A	J	K	L	M	N	O	P	Q
1	End-User	Password_cracked_b	Phishing_a	Browse time_a (22/09/20	Browse time_a (23/10/20(	Password_cracked_a	TEST SCORE 1	TEST SCORE 2	TEST SCORE 3
19	3308	N	Y	567	618	N	7	5	4
60	9691	N	N	153	18	N	6	5	4
81	8030	N	Y	21	75	N	7	5	5
103	7192	N	Y	1803	1662	N	5	3	4
135	3237	N	N	2004	1965	N	7	5	3
150	2843	Y	N	#N/A	#N/A	N	7	4	5
183	284	N	Y	2229	#N/A	N	4	5	5
188	2870	N	Y	1800	780	N	7	4	3
200	2547	N	N	1059	453	N	7	5	4
278	1856	Y	N	756	852	N	7	3	3
302	5655	N	Y	6	81	N	6	5	3
313	539	Y	N	12	504	N	7	5	4
326	379	N	N	120	105	N	4	4	3
342	4732	Y	Y	255	399	Y	4	5	5
359	5999	Y	N	183	312	N	5	5	4
366	5756	Y	Y	54	663	N	6	4	3
379	6231	N	N	6	2121	N	7	5	3
385	5760	Y	N	4680	#N/A	N	6	5	5
390	1479	Y	Y	#N/A	174	N	6	4	4
422	2425	N	Y	252	420	N	6	3	4
448	6228	Y	N	996	345	Y	7	5	3
463	6865	N	Y	3870	4677	N	7	4	3
465	7372	N	Y	192	96	N	7	3	3
489	9420	N	Y	660	846	N	6	5	2
516	69	Y	Y	114	540	Y	6	4	4
630	598	N	N	1362	1101	N	7	4	5
653	158	N	N	111	345	N	5	4	5
684	3270	Y	N	603	3	N	7	3	4
687	800	N	Y	243	237	N	7	5	3
700	3041	Y	Y	#N/A	#N/A	N	6	5	4
702	6382	N	Y	42	#N/A	N	6	5	4
719	683	Y	N	81	483	N	7	5	5
810	5504	Y	Y	2769	#N/A	N	7	5	3

Figure 4: Security scorecard

The research design allows various relationships to be measured. In terms of hypothesis 1a and 1c the differences are measured between the control and the experimental groups using a chi-square test. Thus differences will be observed for Naïve Mistakes and Basic Hygiene.

3.2.4 The effect of the information security awareness strategy

The security awareness material consisted of a professionally commissioned security awareness film for which a script was written. This script was based on Topaz CC's AUP and the existing security guideline booklet. The script was then performed by professional actors and filmed at Topaz CC's premises so that end-users would be able to relate to the environment when viewing the film. The actual film was created in three parts each of which contained a specific theme for the end-users. The theme for part one of the film was Passwords, Clean Desk and Information Handling, part two of the film was on Malicious Code, Virus Protection and Software Use Part three of the film depicted Mobile computing, Internet and e-mail use, storage use and inappropriate content. The method chosen to screen the film to the users was by means of streaming video coupled to a competition.

In order to test hypothesis 2 – End-user exposure to security awareness training increases the internalisation of security knowledge – it was necessary that the end-users' understanding of the security material (three-part security awareness film) be tested by way of a security test. Accordingly the training material was designed in the following way:

1. A competition was announced to both the control and the experimental group members.
2. The competition was divided into three parts and it ran over a number of weeks. In order to stand a chance of winning, each participant had to participate in each section of the competition.
3. The experimental group members were requested to watch each part of the film and they were then asked a series of questions that would both test their comprehension (knowledge questions) and gauge their opinion on the value of the film.
4. The control group was not exposed to the three parts of the film and they were merely directed to the three sets of questions to test their comprehension.
5. After the third and final part of the competition had been deployed the winner of the competition was announced.

The training material was designed to use techniques borrowed from learning science and related disciplines to ensure that that it was as effective as possible. As was discussed in the previous chapter previous researchers have also found the use of a film in a training environment to be an effective tool in rendering the message more appealing to audiences (Mitnick & Simon, 2002:250; Hansche et al., 2004:68). In addition, the training material and its implementation were compatible with the properties of a successful security awareness campaign.

Hansche et al. (2004:71), for example, argue that, for any awareness programme, the awareness messages should, inter alia, be simple and straightforward, and be positive and motivational. It should entertain the audience, be humorous where appropriate, convey to the audience what the threats comprise and what their responsibilities are and reiterate the most important messages. To this end the awareness film deployed in this research meets and even exceeds these requirements. The film was written to be entertaining and to create an absorbing story by depicting humorous scenarios and even perhaps extreme situations. Key messages were repeated by the actors and subtitles were included during important events in the story. Actors were portrayed in difficult scenarios often faced by employees at Topaz CC. Initially the actors were shown performing inappropriate behaviour and the risks of such forms of behaviour were explained. Thereafter the appropriate behaviours were depicted by the actors thus portraying to the audience the behaviour that is expected of them. Thus the film provided context as well as the necessary content required.

Acclimation is one condition that afflicts certain awareness campaigns and it is a condition that must be avoided at all costs. In terms of acclimation a stimulus which is designed to be an attention getter is used repeatedly with the result that the learner will selectively ignore the stimulus. For the purpose of this research it is unlikely that such a situation arose since the research participants were exposed to the specific security awareness material only once. However, in the long-term, organisations using awareness techniques are challenged to devise something new and innovative in order to capture and to hold the attention of the participants.

Finally, as was previously mentioned, both the control group and the experimental group members had to complete three security tests which were designed to measure their understanding of the AUP. Thus, the first test assessed the understanding of password usage and information handling. Accordingly a high score for this test would mean that the participants had a good understanding of what is required in terms of information handling and password usage from a policy point of view. The second test assessed the participants' understanding of malicious code and software usage policy. The third test assessed the end-users' understanding of Internet and Email usage policy.

Table 7: Hypothesis 2 mapped to variables

Hypothesis Description	*Indep. variable*	*Dependent Variable Measurement*	*Analysis*	*Dependent Variable Score Calculation*
H2: End-user exposure to security awareness training increases the internalisation of security knowledge	Binary: Viewed security awareness film (Y or N)	A numerical variable was used. Control and experimental group members were required to answer a set of questions after each part of the film.	Independent -samples t test and Mann-Whitney test.	Multiple choice questions were presented. Each correct answer was awarded a score of 1. Each incorrect score was awarded a value of zero. Scores for each part of the survey part were tallied in order to obtain 3 scores for each end-user.

In terms of hypothesis 2 once again a difference was sought between the scores of the control and the experimental groups for each of the tests using an independent-samples t test and a Mann-Whitney test where appropriate. Since both the control and the experimental group members each completed three separate tests these test scores were compared to ascertain whether there were any significant differences between the control and the experimental groups. An overall difference between the control and the experimental groups was expected, namely, that the control group scores would be lower than the scores of the experimental group since the experimental group had undergone training.

In terms of hypothesis 3 a test was carried out to determine whether there was a significant difference between the mean test scores of the experimental group members and their associated behaviours after training. For example, after training would those experimental group members who had committed Naïve Mistakes score worse on their tests or vice versa. Likewise was there a correlation between the scores obtained by experimental group members and their subsequent Internet browse times? One would expect there to be a strong correlation between high scores (for control and experimental groups) and Internet browse times. This would then have supported the hypothesis which is depicted in table 8 below.

Table 8: Hypothesis 3 mapped to variables

Hypothesis Description	*Indep. variable*	*Dependent Variable Measurement*	*Analysis*	*Dependent Variable Score Calculation*
H3: Internalised security information is necessary for users to enact appropriate security behaviours.	Test scores for each of the three tests under-taken by users.	See dependent variable measurement for H1a, H1b and H1c above.	Independent -samples t test, Spearman Rank Order Correlation.	See dependent variable calculation for H1a, H1b and H1c above.

3.3 SUMMARY

This chapter presents a detailed research strategy which illustrates the way in which this research was carried out in order to achieve those objectives which were introduced in chapter 1, namely, to determine the impact of information security awareness training on information security behaviour. The approach was divided into two strategies. The first strategy concerned hypothesis one and portrayed the way in which the variables in this hypothesis were operationalised using system-generated data. The strategy was depicted in terms of sampling, data collection and data analysis activities. A subset of behaviours (based on a typical Acceptable Usage Policy) that require low technical expertise on the part of the end-user only were considered to be in scope. The second strategy covered hypotheses two and three and focused on the awareness material and the way in which this material was designed, deployed and measured in terms of sampling, data collection and data analysis.

CHAPTER 4 : PRESENTATION OF RESULTS AND INTERPRETATION

We are not in the business of protecting information. We only protect information in so far as it supports the business needs and requirements of our company

Senior Security Manager at a major electric utility (GAO, 1998:21)

The purpose of this chapter is to present the results of the statistical techniques which were employed in respect of the hypotheses, the research problem which was introduced in chapter 1 and the literature survey which was presented in chapter 2. Thus the meaning and implications of these statistical techniques will be explained in light of the objectives of this research and will take into account the theoretical model proposed by this research report.

4.1. PILOT STUDY RESULTS

Essentially two pilot studies were carried out before the deployment of the security awareness training at Topaz CC. A "pre-pilot" test was carried out on the 29 November 2007. It was deployed to employees of the organisation in order to gauge their response to the awareness material. The pre-pilot test comprised the screening of the first part of the security awareness film in an auditorium to a captive audience of 53 individuals during their induction training. This pre-pilot test lasted 25 minutes – 15 minutes to view the film and 10 minutes during which questions were fielded and the audience completed the questionnaire. Four simple questions were posed to the audience. Two of the questions were in respect of their perception of the awareness movie while the other two comprised knowledge questions to test the comprehension of the material in the film. Overall the responses were positive:

- 51 individuals responded (returned the questionnaire) – 96.2%
- 100% of the audience agreed that the film had provided clarity in respect of what is expected of them in terms of security
- 98% of the audience (50 responses) responded that they learnt something new from viewing the film
- No negative comments were received except one to the effect that the questionnaire could have been more simple
- Knowledge question 1: 92% answered correctly
- Knowledge question 2: 94% answered correctly

The purpose of the pre-pilot study was to obtain a response to the film and to ensure that the message in the film was comprehensible to the members of the audience.

The actual pilot study commenced on 28 May 2008 and ended on 13 June 2008. This study consisted of showing the three part security awareness film and then administering the accompanying security test to 17 individuals within the organisation. In order to obtain a broad spectrum of opinions for the pilot study the individuals selected were not members of the same department. They were requested to watch the film and to answer the accompanying questions. They were specifically instructed to highlight any questions that were ambiguous or which were open to misunderstanding. Ten individuals responded to this request. All of the respondents were of the opinion that the questions were clear and to the point and, apart from a few grammatical changes, the actual research design did not materially change. It was decided to deploy the awareness material in its present form.

As mentioned previously the sample was based on those users who had Internet access. The control group and the experimental group were split evenly with 1,072 of the sample in the control group and the other half in the experimental group. Within the organisation there are 3 divisions that are considered to be technical divisions. In other words, these divisions are focused on the developing, managing and maintaining of the IT systems for Topaz CC. Therefore employees in the organisation who are members these divisions are considered "technical" as opposed to "non-technical". For example, a system administrator in the IS division in the IT department is considered to be technical, whereas a financial controller in the finance division is considered as non-technical. The split of end-users in the sample is presented in figure 5 below – 30% (639) of end-users are considered technical whereas 70% (1,505) are considered non-technical.

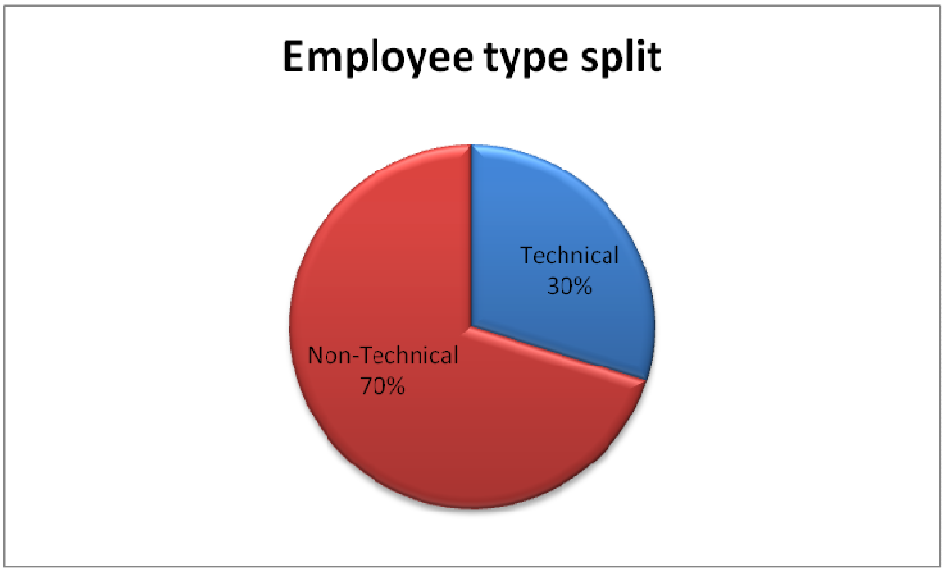


Figure 5: Technical vs. Non-technical split within sample

The entire sample consisted of users within the South African operations which are geographically dispersed across the country. Job types varied across divisions and ranged from senior managers to call-centre agents and system administrators. Employees within the sample also enjoyed different types of employment relationships with Topaz CC:

Table 9: Employment types within the sample showing permanent vs. non-permanent split

Employee category	Count (%)
Permanent employee	1557 (73%)
Non-permanent employee (includes: contractors, temporary workers, consultants and outsourced employees)	587 (27%)
Total	2144 (100%)

4.2. RESULTS OF SECURITY BEHAVIOUR MEASUREMENT STRATEGY

4.2.1. Sampling

4.2.1.1. Naïve Mistakes

In terms of Naïve Mistakes (H1a) the phishing email which had been devised was sent to the entire sample of 2,144 end-user email addresses prior to the end-users undergoing training. The phishing email was sent on Saturday, 26 July 2008. The last response to the phishing email was received on 30 July 2008 at 20:00. One of the participants interfered with the study and attempted to poison the results by sending fabricated data to the server which was collating the information. The worst case scenario was assumed and 6 responses were discarded from the list of responses. Therefore, the response rate totalled 1,138 hits or 53% of the sample.

In terms of the post-security awareness deployment the same phishing email was sent to the same sample as before on Monday, 8 September 2008. The last response to the phishing email was received on 20 October 2008. The response rate was 1,004 hits or 47%. In order to place this response rate in perspective Jagatic et al. (2007) carried out context-aware phishing tests and obtained a hit rate of 74%.

Security test 1 measured Naïve Mistakes and, therefore, only those experimental members who had completed part 1 of the training and the security test were taken into account. A total of 57 experimental group members responded to the 1st part of the training while 221 control group members responded to the 1st survey. This amounts to a response rate of 5% and 20% respectively. Consequently, this was the final sample size used in the statistical analysis.

4.2.1.2. Detrimental Misuse

The SurfControl web filtering tool was used to gather Internet browse times for both the control and the experimental group members. Two extracts were taken – one before and one after the security awareness intervention. The first extract was generated on 15 July 2008 for the period 1 July 2008–15 July 2008 while the second extract was generated on 22 September 2008 for the period 8 September 2008 – 22 September 2008.

In terms of the pre-security awareness extract 2 070 records were obtained – a 97% response rate while for the post-security awareness extract 1,710 records of the sample groups were obtained.

4.2.1.3. Basic Hygiene

As a result of the fact that Windows Active Directory (AD) passwords has the greatest coverage of users this application was chosen as the end-user passwords to be tested for password strength. The password hashes were extracted on 27 June 2008 for purposes of the pre-security awareness test.

In total 20,447 password hashes were extracted from AD. The vast majority of these hashes were system accounts and other irrelevant accounts that were subsequently discarded. Of the 2,144 passwords in scope, 1,180 passwords hashes were either partially cracked or not cracked at all. Therefore a total of 964 passwords were fully cracked. A further 42 user accounts had a "NO PASSWORD" in the password hash field which signifies a problem with the password hashes at the time of the data gathering. The latter had to be discounted with the result that the final list of passwords that could be fully cracked totalled 922 passwords – 43% of the control and experimental group passwords.

Password cracking after the security awareness intervention took place in the following way. The password hashes were extracted and cracked on 20 September 2008. The passwords were cracked as before using the same level of processing power and the same rule set Of the 2,144 passwords in scope 1,762 passwords where either partially cracked or not cracked at all. Therefore the remaining passwords that were fully cracked totalled 382 passwords. A further 48 user accounts had "NO PASSWORD" in the password hash field which signifies that there was a problem with the password hashes at the time of the data gathering. The latter has to be discounted with the result that the final list of passwords that could be fully cracked totalled 334 passwords – 16% of all the control and experimental groups. This represents a 27% improvement in the strength of passwords overall.

4.2.2. Data collection

4.2.2.1. Naïve Mistakes

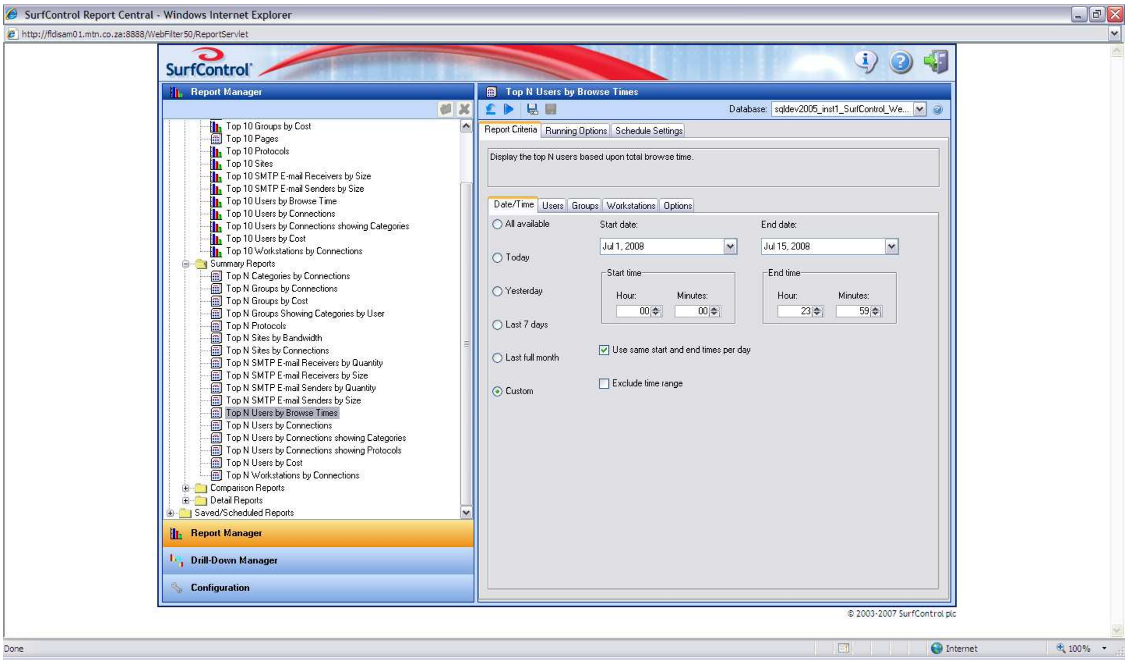
As mentioned above, in order to test Naïve Mistakes, a phishing email was sent to the sample, *n*, both before and after the security awareness training intervention to determine whether the awareness intervention had made a difference. The method used to gather the data was simple. Each sample member received the email in his/her inbox. The email contained a hyperlink that, when clicked, would establish a connection to a server on the Internet and register that particular email address. A log of all those users who clicked on the link successfully ("hit list") was then extracted and matched against the list in the sample (targets). If the user had clicked on the link a "Y" was inserted in the phishing column, otherwise an "N" was inserted in the phishing column of the security behaviour scorecard. The researcher double checked to ensure that those users with "Y" against their names were members of the "hit list" and that those with an "N" against their names were not on the "hit list" – this was done by carrying out random spot checks. In terms of the post security awareness training phishing email the design was changed slightly to avoid the attempted sample poisoning that had occurred in the first round. For this round hashes were used to prevent a rogue respondent from generating false responses.

The data gathered for Naïve Mistakes were populated in the security behaviour scorecard of each sample member for further analysis.

4.2.2.2. Detrimental Misuse

SurfControl is a commercially available software tool that Topaz CC had purchased and which had been in operation in the organisation for a period of three years. It is installed on the organisation's proxy server and, therefore, it monitors all Internet (and Intranet) bound traffic. All internal workstations requesting Internet connections are forced to connect via this proxy. Thus all Internet traffic is logged by SurfControl. SurfControl's standard reports, such as the top ten sites visited and the top ten users by browse time have, in the past, been used by the organisation. The browse times for the purposes of this research were generated and displayed as total minutes for the period in question (2 weeks) per user.

The following screenshot represents the SurfControl reporting interface which was used to generate a "Top N Users by Browse Time" report.



SurfControl Report Central - Windows Internet Explorer

http://fldisam01.mtn.co.za:8888/WebFilter50/ReportServlet

Report Manager

- Top 10 Groups by Cost
- Top 10 Pages
- Top 10 Protocols
- Top 10 Sites
- Top 10 SMTP E-mail Receivers by Size
- Top 10 SMTP E-mail Senders by Size
- Top 10 Users by Browse Time
- Top 10 Users by Connections
- Top 10 Users by Connections showing Categories
- Top 10 Users by Cost
- Top 10 Workstations by Connections
- Summary Reports
  - Top N Categories by Connections
  - Top N Groups by Connections
  - Top N Groups by Cost
  - Top N Groups Showing Categories by User
  - Top N Protocols
  - Top N Sites by Bandwidth
  - Top N Sites by Connections
  - Top N SMTP E-mail Receivers by Quantity
  - Top N SMTP E-mail Receivers by Size
  - Top N SMTP E-mail Senders by Quantity
  - Top N SMTP E-mail Senders by Size
  - Top N Users by Browse Times
  - Top N Users by Connections
  - Top N Users by Connections showing Categories
  - Top N Users by Connections showing Protocols
  - Top N Users by Cost
  - Top N Workstations by Connections
- Comparison Reports
- Detail Reports
- Saved/Scheduled Reports

Top N Users by Browse Times

Database: sqldev2005_inst1_SurfControl_We...

Report Criteria | Running Options | Schedule Settings

Display the top N users based upon total browse time.

Date/Time | Users | Groups | Workstations | Options

○ All available
○ Today
○ Yesterday
○ Last 7 days
○ Last full month
● Custom

Start date: Jul 1, 2008

End date: Jul 15, 2008

Start time — Hour: 00 Minutes: 00

End time — Hour: 23 Minutes: 59

☑ Use same start and end times per day

□ Exclude time range

© 2003-2007 SurfControl plc

Figure 6: SurfControl reporting interface

4.2.2.3. Basic Hygiene

Two steps were followed in the collection of the data. First a tool known as *pwdump3e* was used to extract password hashes from Active Directory. Once this had been completed the password hashes were subjected to a password cracking exercise to find out whether they appeared in a wordlist (or represented a variation of an entry in the wordlist). As mentioned, the password cracker used is termed *John the Ripper* (*John*). The crack ran for 3 minutes with a dictionary list of 43 MBs with the word mangling option enabled. The hardware used comprised a standard laptop with 2GB of RAM and a 2Ghz Intel Core Duo CPU. The options selected – wordlist and mangling – simply mean that all the words and common phrases that appear in the wordlist are compared against the extracted password hashes to determine whether there is a match. If there is match the program, *John*, will display the discovered password alongside the extracted username. With word mangling enabled variations of the words and phrases in the wordlist are generated and compared with the extracted password hashes.

If *John* is able to find a partial password then it will display letters in the password that it could find and the ones that it could not find will be indicated by a "?". Therefore, assuming that *John* is attempting to crack the password – AdidasG254$ – and that it is able to find the first 6 letters only then the following would be displayed: Adidas?????. This would then be considered an uncracked password.

All passwords that were fully cracked were designated by a "Y" next to the relevant user name on the security behaviour scorecard and an "N" if not fully cracked.

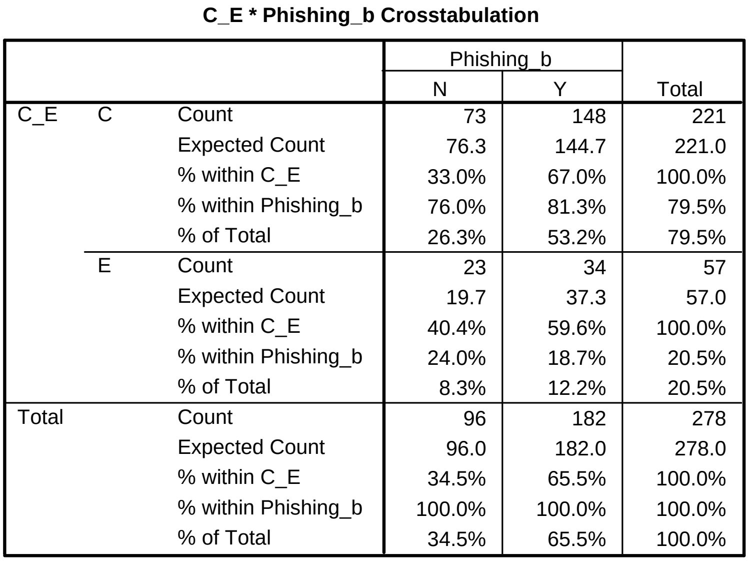
4.2.3. Data analysis

In view of the fact that the intention was to explore the relationship between two categorical variables a Chi-Square test for independence was used for Naïve Mistakes and Basic Hygiene. For Detrimental Misuse an independent-samples t test was used.

4.2.3.1. Naïve Mistakes

The sample consisted of an experimental group of 57 end-users and a control group of 221 end-users. As illustrated in table 10 below, prior to the training intervention, 67% of the control group members were non-compliant (taken in by a phishing attack) as opposed to 59.6% of the experimental group members.

Table 10: Summary of Naïve Mistakes results before training for control vs. experimental groups



C_E * Phishing_b Crosstabulation

			Phishing_b		
			N	Y	Total
C_E	C	Count	73	148	221
		Expected Count	76.3	144.7	221.0
		% within C_E	33.0%	67.0%	100.0%
		% within Phishing_b	76.0%	81.3%	79.5%
		% of Total	26.3%	53.2%	79.5%
	E	Count	23	34	57
		Expected Count	19.7	37.3	57.0
		% within C_E	40.4%	59.6%	100.0%
		% within Phishing_b	24.0%	18.7%	20.5%
		% of Total	8.3%	12.2%	20.5%
Total		Count	96	182	278
		Expected Count	96.0	182.0	278.0
		% within C_E	34.5%	65.5%	100.0%
		% within Phishing_b	100.0%	100.0%	100.0%
		% of Total	34.5%	65.5%	100.0%

As shown in table 11 below chi-square indicates that there is no significant difference between the percentage of non-compliant members in the control group and the percentage in the experimental group. The continuity correction value is .774 with an associated significance level of .379 which is > .05.

Table 11: Chi-Square test results for Naive Mistakes before training

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.074[b]	1	.300		
Continuity Correction[a]	.774	1	.379		
Likelihood Ratio	1.055	1	.304		
Fisher's Exact Test				.349	.189
N of Valid Cases	278				

[a] Computed only for a 2x2 table

[b] 0 cells (.0%) have expected count less than 5. The minimum expected count is 19.
68.

The results of both the control group members and the experimental group members after the training show that there was an improvement in the behaviour towards the phishing email (Naïve Mistakes) in both groups. The more marked improvement was noted within the control group segment with 53.4% non-compliant (down from 67%) while 57.9% of the experimental group members were non-compliant (down from 59.6%). The results are presented in table 12.

Table 12: Summary of Naïve Mistakes results after training for control vs. experimental groups

C_E * Phishing_a Crosstabulation

			Phishing_a		
			N	Y	Total
C_E	C	Count	103	118	221
		Expected Count	101.0	120.0	221.0
		% within C_E	46.6%	53.4%	100.0%
		% within Phishing_a	81.1%	78.1%	79.5%
		% of Total	37.1%	42.4%	79.5%
	E	Count	24	33	57
		Expected Count	26.0	31.0	57.0
		% within C_E	42.1%	57.9%	100.0%
		% within Phishing_a	18.9%	21.9%	20.5%
		% of Total	8.6%	11.9%	20.5%
Total		Count	127	151	278
		Expected Count	127.0	151.0	278.0
		% within C_E	45.7%	54.3%	100.0%
		% within Phishing_a	100.0%	100.0%	100.0%
		% of Total	45.7%	54.3%	100.0%

As illustrated in table 13 below the chi-square test after the training for Naïve Mistakes indicates that there are no significant differences between the control group and the experimental group. Improvements were noted in both groups. This means that the Naïve Mistakes on the part of those end-users who underwent security training do not differ significantly from those who did not undergo the awareness training.

Table 13: Chi-Square test results for Naive Mistakes after training

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.370[b]	1	.543		
Continuity Correction[a]	.211	1	.646		
Likelihood Ratio	.371	1	.542		
Fisher's Exact Test				.555	.324
N of Valid Cases	278				

[a] Computed only for a 2x2 table

[b] 0 cells (.0%) have expected count less than 5. The minimum expected count is 26. 04.

The continuity correction value is .211 with an associated significance level of .646 which is > .05.

4.2.3.2. *Detrimental Misuse*

The sample of Detrimental Misuse behaviours consisted of 17 end-users in the experimental group and 86 end-users in the control group. In other words, this is the amount of responses received for the third security test which was completed by both the experimental and control group members. The third security test relates to Detrimental Misuse behaviour (for example acceptable Internet usage) thus only those control and experimental group members who had been exposed to this particular training and security test were taken into account. Browse time information for some users could not be obtained from the SurfControl tool, and this resulted in the final *N* values depicted below.

Table 14: Descriptive Statistics for control and experimental groups for browse time before and after training

Group Statistics

	C_E	N	Mean	Std. Deviation	Std. Error Mean
Browse_time_b	C	80	682.050	1206.0019	134.8351
	E	17	487.235	617.1174	149.6730
Browse_time_a	C	74	866.230	1200.4533	139.5499
	E	14	612.429	1167.0026	311.8946

Table 15: Independent-Samples t test results for Detrimental Misuse

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Browse_time_b	Equal variances assumed	.736	.393	.646	95	.520	194.8147	301.3955	-403.5311	793.1605
	Equal variances not assumed			.967	46.328	.339	194.8147	201.4510	-210.6077	600.2371
Browse_time_a	Equal variances assumed	.281	.597	.728	86	.468	253.8012	348.4138	-438.8226	946.4249
	Equal variances not assumed			.743	18.593	.467	253.8012	341.6905	-462.4256	970.0279

As may be seen in the table above the differences between the mean browse times (Detrimental Misuse) of the control and the experimental groups before the training intervention was not significant (t= .646, p > .05). Likewise, after the training there was no significant difference between the experimental and the control groups end-users in terms of Detrimental Misuse (t = .728, p > .05).

4.2.3.3. Basic Hygiene

The sample consisted of 57 end-users in the experimental group and 221 end-users in the control group. As is illustrated in table 16, before the training intervention, it was possible to crack 46.6% of the control group members' passwords and 36.8% of the experimental group members' passwords.

Table 16: Summary of Basic Hygiene results before training for control vs. experimental groups

C_E * Password_Cracked_b Crosstabulation

			Password_Cracked_b		
			N	Y	Total
C_E	C	Count	118	103	221
		Expected Count	122.4	98.6	221.0
		% within C_E	53.4%	46.6%	100.0%
		% within Password_ Cracked_b	76.6%	83.1%	79.5%
		% of Total	42.4%	37.1%	79.5%
	E	Count	36	21	57
		Expected Count	31.6	25.4	57.0
		% within C_E	63.2%	36.8%	100.0%
		% within Password_ Cracked_b	23.4%	16.9%	20.5%
		% of Total	12.9%	7.6%	20.5%
Total		Count	154	124	278
		Expected Count	154.0	124.0	278.0
		% within C_E	55.4%	44.6%	100.0%
		% within Password_ Cracked_b	100.0%	100.0%	100.0%
		% of Total	55.4%	44.6%	100.0%

Chi-square indicates that that there is no significant difference between the percentage cracked in the control group and the percentage cracked in the experimental group. As shown in table 17 below the continuity correction value is 1.376 with an associated significance level of .241.

Table 17: Chi-Square test results for Basic Hygiene before training

Chi-Square Tests

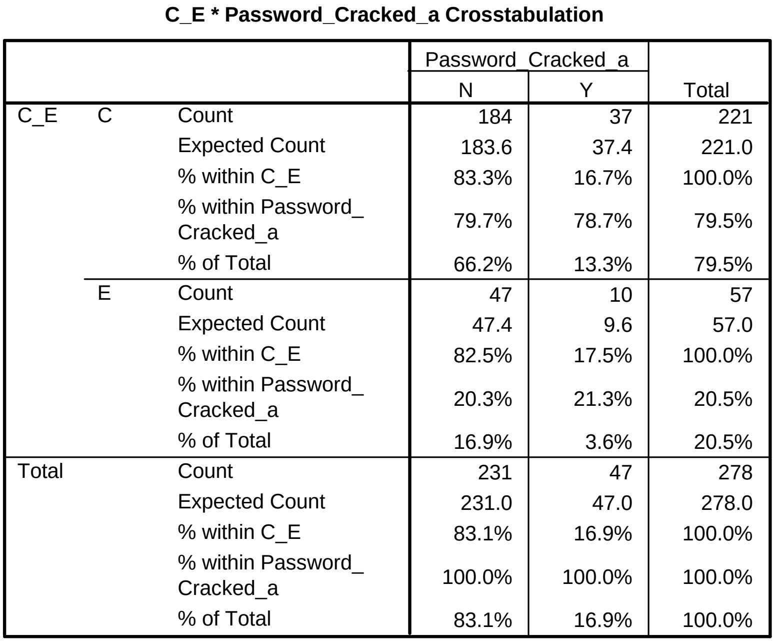
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.748[b]	1	.186		
Continuity Correction[a]	1.376	1	.241		
Likelihood Ratio	1.769	1	.183		
Fisher's Exact Test				.232	.120
N of Valid Cases	278				

a. Computed only for a 2x2 table

b. 0 cells (.0%) have expected count less than 5. The minimum expected count is 25.
42.

The results obtained after the training indicated that there had been a dramatic improvement in terms of both the control group members and the experimental group members as it was possible to crack 16.7% only of the control group member passwords (down from 46.6%) while 17.5% only of the experimental group member passwords could be cracked (down from 36.8%).

Table 18: Summary of Basic Hygiene results after training for control vs. experimental groups

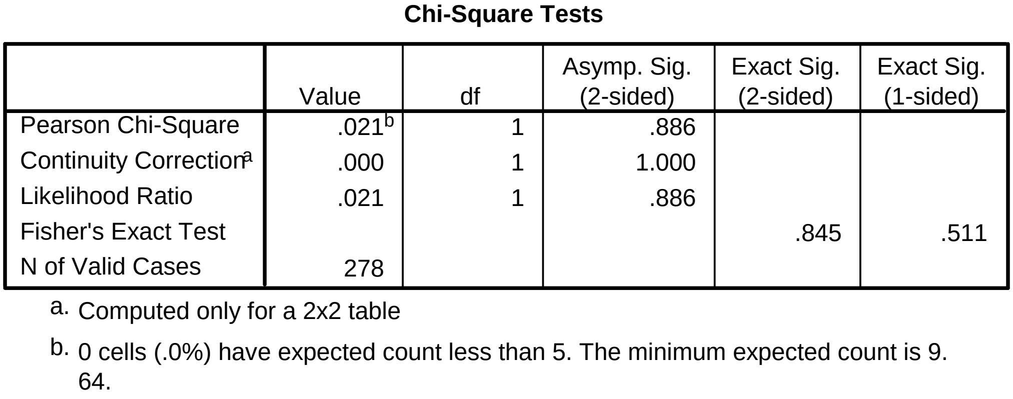


C_E * Password_Cracked_a Crosstabulation

			Password_Cracked_a		
			N	Y	Total
C_E	C	Count	184	37	221
		Expected Count	183.6	37.4	221.0
		% within C_E	83.3%	16.7%	100.0%
		% within Password_ Cracked_a	79.7%	78.7%	79.5%
		% of Total	66.2%	13.3%	79.5%
	E	Count	47	10	57
		Expected Count	47.4	9.6	57.0
		% within C_E	82.5%	17.5%	100.0%
		% within Password_ Cracked_a	20.3%	21.3%	20.5%
		% of Total	16.9%	3.6%	20.5%
Total		Count	231	47	278
		Expected Count	231.0	47.0	278.0
		% within C_E	83.1%	16.9%	100.0%
		% within Password_ Cracked_a	100.0%	100.0%	100.0%
		% of Total	83.1%	16.9%	100.0%

As shown below in table 19 no significant difference exists between the two-groups in terms of Basic Hygiene (password strength). The continuity correction value is .000 with a significance level of 1.000. This means that the Basic Hygiene behaviour of those end-users who underwent security training did not differ significantly from those who had not undergone the awareness training although it was possible to see improvements in both groups.

Table 19: Chi-Square test results for Basic Hygiene after training



Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.021[b]	1	.886		
Continuity Correction[a]	.000	1	1.000		
Likelihood Ratio	.021	1	.886		
Fisher's Exact Test				.845	.511
N of Valid Cases	278				

[a] Computed only for a 2x2 table

[b] 0 cells (.0%) have expected count less than 5. The minimum expected count is 9. 64.

4.3. RESULTS OF THE INFORMATION SECURITY AWARENESS STRATEGY

4.3.1. Sampling

As has already been mentioned the awareness training material consisted of a film in three parts and security tests that were administered to the experimental group. The control group had to complete three security tests. Neither group was given the correct answers to the tests. Both groups were eligible to take part in the competition. The first part of the competition was announced to both the control and the experimental group members on the 31st July 2008 and it continued throughout August and the first week of September 2008. The awareness deployment closed on the 10th September 2008 and the winner of the competition was announced on the same day.

For all three parts of the competition the users were invited to participate. In order to be considered eligible to win one of the prizes the experimental group members had to view the relevant part of the film (by clicking on the hyperlink provided) and complete the security test. In order to stand a chance of winning the control group had to complete all three security tests. Consequently, the samples were not equal probably as a result of the fact that it was easier for the control group members both to enter and to take part in the competition than it was for the experimental group members.

The three parts of the competition (corresponding to the three parts of the awareness movie and security tests) were administered as follows:

- Part 1administered to both groups on 31 July 2008
- Part 1 reminder administered to both groups on 8 August 2008
- Part 2 administered to both groups on 21 August 2008
- Reminder email sent on 2 September 2008
- Part 3 administered to both groups on 5 September 2008.

All group members had to register on a web interface in order to take part in the competition. In practice this meant that once the end-user has clicked on the link provided in the email communiqué he/she would need to fill in email address, name and surname. Thereafter the end-user was directed to the awareness film (if a member of the experimental group) or the applicable security test (if a member of the control group). Although 841 end-users had registered to take part in the competition not all the responses were valid. There were a number of reasons for this fact, for instance, certain end-users: were not in scope (not members of either the control or the experimental group), certain end-users registered but did not complete the necessary security test (some completed part 1 but not part 2), they supplied incomplete/incorrect information or they submitted multiple completed security tests. After all the invalid and the duplicate responses had been discarded the following valid sample remained.

Table 20: Valid responses obtained from questionnaires

	Test 1	Test 2	Test 3
Control Group	221	142	86
Experimental Group	57	30	17
Total responses	258	172	103

4.3.2. Data collection

A custom-built web interface with a Microsoft Access database on the back-end for storing the necessary data was used to collect the end-user test responses. The data was stored in individual fields that could be extracted for later analysis. Each participant was referenced by his/her email address. Each row within the database contained the email address of the end-user, whether the end-user had been in the control group or the experimental group and the answers for each question in the tests. Each correct score was awarded one point. Thereafter, the score per test was populated in the security behaviour scorecard.

4.3.3. Data Analysis

In terms of hypothesis 2 the test scores of both the control and the experimental group members were compared to determine whether the experimental group members had fared better than the control group members. For test scores 1, 2 and 3 the data analysis sections below describe, firstly, the basic features of the statistics, and, secondly, the results of the t-tests and the Mann-Whitney test.

4.3.3.1. Test score 1 results

For test score 1, which assesses comprehension in terms of Naïve Mistakes (information handling) and Basic Hygiene (password strength), the mean for the control group was 5.90 with a standard deviation of 1.141. This produced a range of scores between 4.755 and 7.037 in which two-thirds of the scores fell. For the experimental group the mean was slightly higher at 6.357 with a standard deviation of 0.862. This produced a range of scores from 5.495 to 7.219 in which two-thirds of the sample fell. The standard deviation was considered relatively small and this points to overall consensus in terms of the questions. *n* was 278 (221 control group members and 57 experimental group members).

The distribution of the results, together with a normal curve for test 1 results, is presented in figure 7 shown.

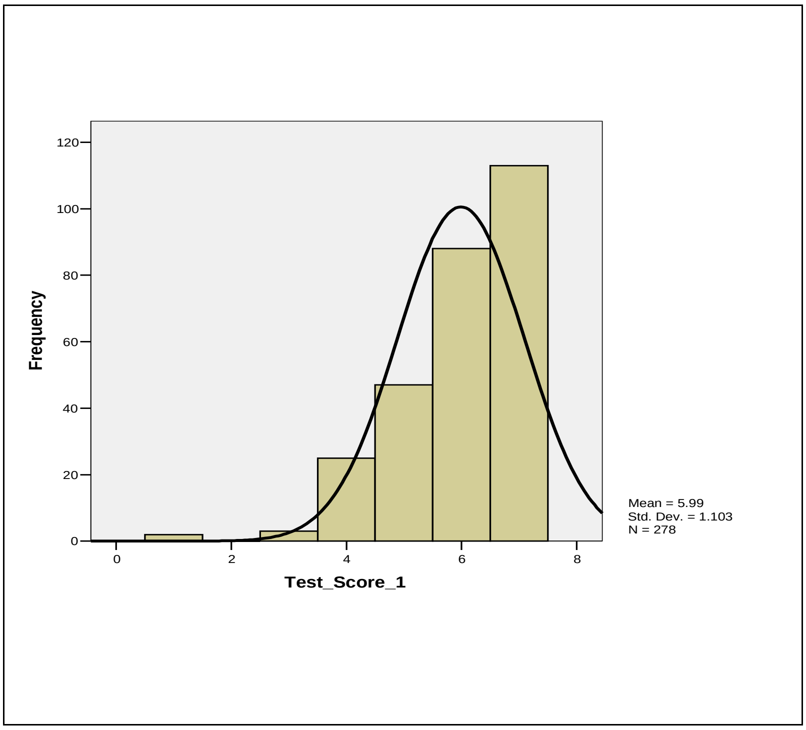
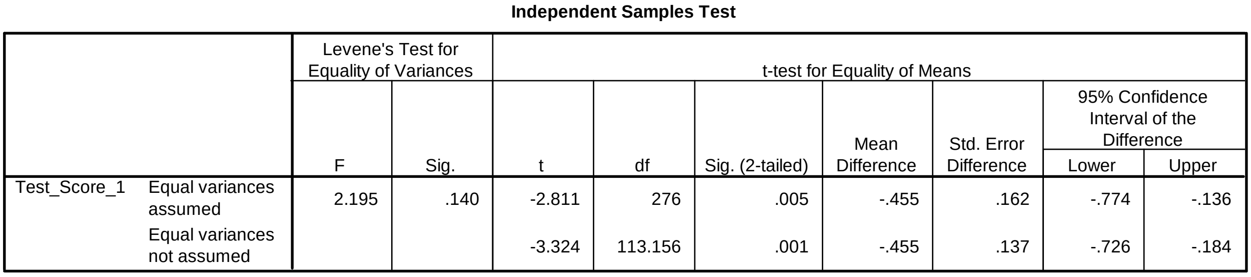


Figure 7: Distribution of test 1 results

The Skewness value is -1.231 and the Kurtosis is 2.036. As presented in table 21 below the t-test results indicate that the control group scored significantly lower than the experimental group for test 1 (t = -2.811, p < .05).

Table 21: Independent-samples t-test between control and experimental groups for test 1 scores



Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Test_Score_1	Equal variances assumed	2.195	.140	-2.811	276	.005	-.455	.162	-.774	-.136
	Equal variances not assumed			-3.324	113.156	.001	-.455	.137	-.726	-.184

Since there was some concern about the normality of the test 1 scores a Mann-Whitney test was also conducted – the non-parametric alternative to the independent-samples t test (Pallant, 2001:255).

The results of the Mann Whitney test show that for test score 1, on the 1% level of significance, the control group scored less than the experimental group since the *p-value* of 0.002116 < 0.01. Accordingly the results of the t test were confirmed.

4.3.3.2. Test score 2 results

Test 2 measures the understanding of the threats of malicious code and the requirements for proper system and software usage as specified by the AUP. The behaviours associated with this test were not measured in the same way as in the case of the other tests. This test was merely administered to the end-users as part of the overall Information Security Awareness Programme. Nevertheless it is an interesting exercise to look at these results. The mean for the control group was 4.162 with a standard deviation of 0.880. This produced a range of scores between 3.282 and 5.042 in which two-thirds of the scores fell. For the experimental group the mean was somewhat higher at 4.600 with a standard deviation of 0.563. This produced a range of scores from 4.037 to 5.163 in which two-thirds of the sample fell. Both standard deviations are small which, once again, is an indication that the questions posed in the test had not been ambiguous.

The distribution of test 2 results together with a normal curve is shown in figure 8 below. *n* is 172 (142 control group members and 30 experimental group members).

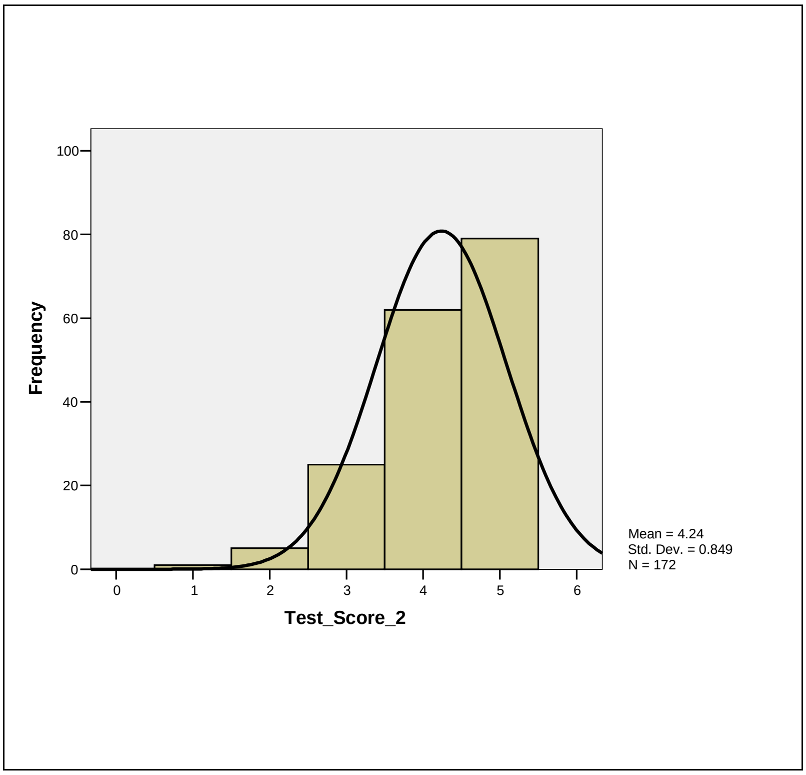


Figure 8: Distribution of test 2 results

The Skewness value is -1.001 and the Kurtosis is.691. Since the Skewness and Kurtosis values are acceptable an independent-samples t test was administered. The results are shown in table 22 below.

Table 22: Independent-samples t test between control and experimental groups for test 2 scores

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Test_Score_2	Equal variances assumed	4.323	.039	-2.611	170	.010	-.438	.168	-.769	-.107
	Equal variances not assumed			-3.459	63.197	.001	-.438	.127	-.691	-.185

As shown above the t-test results indicate that the control group scored significantly lower than the experimental group in terms of test 2 (t = -3.459, p < .05).

4.3.3.3. Test score 3 results

Test 3 measured the understanding of the Internet and Email usage sections of the AUP. The mean of the control group was 3.430 with a standard deviation of 1.035. This produced a range between 2.395 and 4.465. In the case of the experimental group the mean was significantly higher at 4.647 with a standard deviation of 0.606. This created a range from 4.041 to 5.253. The standard deviations were small thus indicating consensus in terms of the questions in the test. The distribution of test 3 results, together with a normal curve, are presented in figure 9 below.

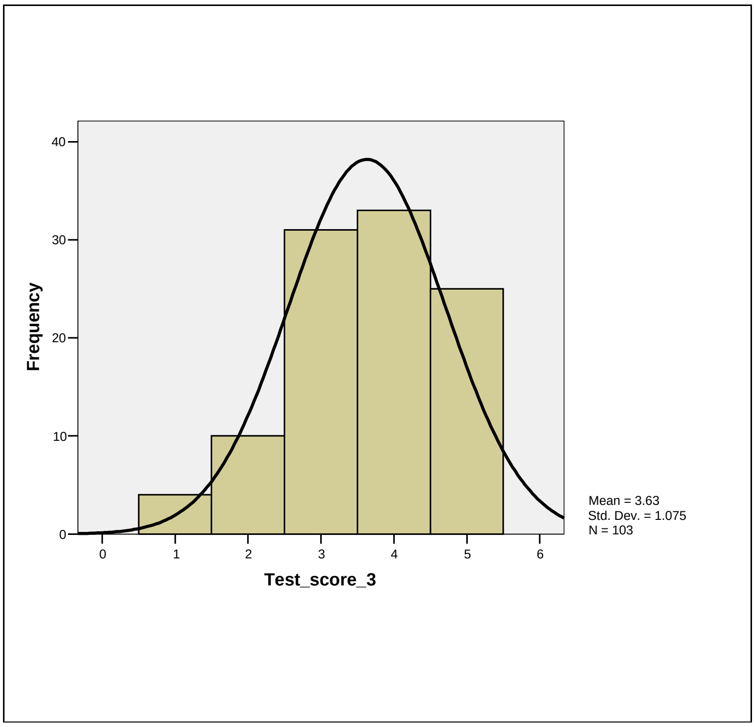


Figure 9: Distribution of test 3 results

The Skewness value is -.468 and the Kurtosis is -.325. Since the Skewness and Kurtosis values are acceptable an independent-samples t-test was administered. The results are presented in table 23 below.

Table 23: Independent-samples t test between control and experimental groups for test 3 scores

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Test_score_3	Equal variances assumed	6.359	.013	-4.679	101	.000	-1.217	.260	-1.733	-.701
	Equal variances not assumed			-6.591	37.410	.000	-1.217	.185	-1.591	-.843

As shown in table 23 above according to the t test results the control group scored significantly lower than the experimental group for test 3 (t = -6.591, p < .05).

4.3.4. Relationship between test scores and behaviours

Hypothesis 3 states that internalised knowledge is necessary for appropriate behaviour to be enacted. In other words, one would expect to see a relationship between test scores (as discussed previously) and the associated behaviours in terms of which a higher test score would be associated with a decrease in Naïve Mistakes, a decrease in Detrimental Misuse and an increase in Basic Hygiene. The experimental group behaviour was divided into positive and negative behaviour and the associated scores for the appropriate test were compared.

The following test scenarios were carried out on the experimental group data which had been obtained after training:

- In terms of Naïve Mistakes did those group members who acted correctly (not be taken in by a phishing scam) obtain a significantly better score for test 1 than those group members who did not act correctly?
- In terms of Basic Hygiene did those group members who acted correctly (chose a strong password) obtain a significantly better score for test 1 than those group members who did not act correctly?
- In terms of Detrimental Misuse did those group members who acted correctly (spent less time browsing) obtain a significantly better score for test 3 than those group members who did not act correctly?

In terms of Naïve Mistakes the mean test score of those group members who did act correctly was 6.42 compared to the score of 6.30 obtained by those group members who did not act correctly. The relevant statistics are presented in table 24 below.

Table 24: Descriptive statistics for experimental group test scores and Naïve Mistakes

Group Statistics

	Phishing_A	N	Mean	Std. Deviation	Std. Error Mean
Test_Score_1	N	24	6.42	.776	.158
	Y	33	6.30	.918	.160

However, the differences in the mean observed are not statistically significantly different as is shown by the following results – t =.492, p > .05.

Table 25: t-test for experimental group test scores and Naïve Mistakes

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Test_Score_1	Equal variances assumed	.458	.501	.492	55	.625	.114	.231	-.349	.577
	Equal variances not assumed			.505	53.689	.616	.114	.225	-.337	.565

Thus, based on these results, it may be concluded that those experimental group members who acted correctly after undergoing training did not obtain a significantly higher test score than those group members who did not act correctly.

In terms of Basic Hygiene those group members who did act correctly obtained a mean test score of 6.28 compared to those who did not act correctly whose score was 6.70. The relevant statistics are presented in table 26 below.

Table 26: Descriptive statistics for experimental group test scores and Basic Hygiene

Group Statistics

	Password_A	N	Mean	Std. Deviation	Std. Error Mean
Test_Score_1	N	47	6.28	.902	.132
	Y	10	6.70	.483	.153

As illustrated in table 27 below significant differences were observed in the mean scores – t= -2.100, p < .05. This statistically significant difference is unexpected and it would appear that a very good understanding of Basic Hygiene does not necessarily ensure that the correct behaviour will be carried out.

Table 27: t-test for experimental group test scores and Basic Hygiene

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Test_Score_1	Equal variances assumed	5.596	.022	-1.435	55	.157	-.423	.295	-1.015	.168
	Equal variances not assumed			-2.100	24.643	.046	-.423	.202	-.839	-.008

In terms of Detrimental Misuse the mean browse time for experimental group members after training was 612.43 minutes. The Skewness level was 3.001 and the Kurtosis level is 9.429. Therefore since the normality of the data is of concern, the non-parametric Spearman Rank Order correlation statistic was used. The outcome of this statistic is presented in table 28 below.

Table 28: Spearman Rank Order Correlation results for the experimental group after training

Correlations

			Browse_ Time_After	Test_Score_3
Spearman's rho	Browse_Time_After	Correlation Coefficient	1.000	-.099
		Sig. (2-tailed)	.	.737
		N	14	14
	Test_Score_3	Correlation Coefficient	-.099	1.000
		Sig. (2-tailed)	.737	.
		N	14	17

As illustrated in table 28 above there appears to be no correlation between the test score results (on Internet acceptable usage) and the actual browse times of end-users in the experimental group after training. A good or bad score obtained for test 3 appears not to be associated in any way with the actual browse time behaviours of end-users. This is further confirmed by the results presented in table 29 below. This table illustrates the results of a Spearman Rank Order correlation test between the control group and the experimental group browse times before training and the control and the experimental group browse times after training. On the 1% level of significance there appears to be a strong correlation between browse times prior to training and after training.

Table 29: Correlation between browse times before and after training.

Correlations

			Browse_ time_b	Browse_ time_a
Spearman's rho	Browse_time_b	Correlation Coefficient	1.000	.693**
		Sig. (2-tailed)	.	.000
		N	97	86
	Browse_time_a	Correlation Coefficient	.693**	1.000
		Sig. (2-tailed)	.000	.
		N	86	88

**. Correlation is significant at the 0.01 level (2-tailed).

4.4. HYPOTHESIS 1: INTERPRETATION OF RESULTS

The first hypothesis is a composite construct which comprises three sub-hypotheses. This first hypothesis states that end-user exposure to security awareness training affects three specific security behaviours in the following ways.

The measurement of information handling was translated into the category of Naïve Mistakes and the susceptibility of end-users to fall for a phishing attack was measured. Based on the data analysis presented previously it may be concluded that the impact of information security awareness training on this particular type of behaviour is not significant in terms of this case study. Improvements were observed in both groups after training. However, in this case it is not possible to attribute the improvement to training alone. It is very likely that the security test written by both groups may have been a factor in influencing the compliant behaviour. As far as the researcher was aware there was no other intervention in terms of these groups. Therefore, based on the data from this research, it is not possible to support this sub-hypothesis. There is no evidence that exposure to security training alone has a positive effect on Naïve Mistakes.

The measurement of acceptable usage of Internet facilities was translated into a Detrimental Misuse category and one variable within this category was measured – total Internet browse times on the part of end-users over a two-week period. Based on the data analysis presented in the previous chapter it was concluded that, despite the lowered mean in the observed behaviour (improved browsed times), the difference between the control and experimental groups before and after the training is not statistically significant. Therefore, the impact of information security awareness training on this particular behaviour is not of any significance for this study. In this case it would appear that exposure to training does not lead to a noticeable improvement in compliant behaviour. Awareness training appears not to be sufficient to ensure end-user security compliant behaviour and, therefore, it is not possible to support this sub-hypothesis.

The measurement of password management best practices was translated into a Basic Hygiene category and one variable, namely, password strength was measured. Based on the data analysis presented earlier it may be concluded that no significant differences between the control and the experimental groups exist. Therefore the impact of information security awareness training on this behaviour is not significant. In this case a dramatic improvement was seen in the password strength of both the control group and the experimental group members. Nevertheless, it would appear that that this improvement was not due only to the training. Awareness training alone appears to be insufficient to ensure end-user security compliant behaviour in this regard and, therefore, this sub-hypothesis is not supported. The likely cause of the improvement in both groups was probably as a result of the fact that both groups had to complete a security test. The test (which did not provide answers to the questions) may have triggered an understanding from prior learning about password strength and thereby reinforced the subsequent compliant behaviour.

Based on the results of these sub-hypotheses it is not possible to support hypothesis 1. However the outcome of this research does not mean that information security awareness training has no impact on information security behaviour. In future multiple variables may have to be examined in order to determine the broader impact of information security awareness training on information security behaviour. The implications are that information security awareness training alone appears to be inadequate to ensure that end-user behaviour is compliant and to prevent non-compliant behaviour (for the behavioural indicators observed). The writing of the security test itself may have had a security effect on the control group by reinforcing prior learning. This is supported by the fact that both groups achieved very high test scores on average.

4.5. HYPOTHESIS 2: INTERPRETATION OF RESULTS

The second hypothesis states that end-user exposure to security awareness training increases the internalisation of security knowledge. The statistical results were presented in the previous chapter. Three sets of scores were examined in terms of this hypothesis — control group and experimental group scores for security tests one, two and three. In each case the control group scores were compared to the experimental group scores.

Based on the results it would appear that, for all the tests undertaken by the control and the experimental group members, the experimental group scored higher than the control group. The implications of this are, firstly, the training seemed to be effective in this case as the end-users in the experimental group fared statistically better than the control group end-users. Therefore, within this specific organisation and based on the sample in this research it would appear that hypothesis 2 is supported by the data presented earlier.

4.6. HYPOTHESIS 3: INTERPRETATION OF RESULTS

The final hypothesis proposes that internalised security information (as measured by hypothesis 2) is necessary for users to enact appropriate security behaviours. Therefore it may be expected that end-users with high test scores would manifest compliant security behaviours. Experimental group end-user data after the members of the experimental group had undergone training was analysed. The following scenarios were examined:

a) In terms of Naïve Mistakes did those whose behaviour was compliant (not fall for a phishing scam) obtain a significantly better score for test 1 than those whose behaviour was not compliant? The results indicate that even though those members of the experimental group who did manifest compliant behaviour obtained a higher mean test score than those who manifested non-complaint behaviour the difference was not statistically significant.

b) In terms of Basic Hygiene did those whose behaviour was compliant (chose stronger passwords) obtain a significantly better score for test 1 than those whose behaviour was not compliant? The results indicate that those members of the experimental group who manifested non-compliant behaviour scored higher in the test than those whose behaviour was compliant. The difference in scores is statistically significant. On the other hand, the group which was compliant had obtained a very high mean score of 90%. In fact, both results (within the experimental group) were very high which implies that internalised knowledge of security may be necessary but is not sufficient to prevent poor security behaviour in this case.

c) In terms of Detrimental Misuse did those who manifested compliant behaviour (spent less time browsing) score better on test 3 than those who manifested non-compliant behaviour? There appears to be no association between better test scores and improved browse times and vice versa.

It may, therefore, be concluded that obtaining a high score is not necessarily an indication of compliant security behaviour. Based on the data from this research it is not possible to support hypothesis 3.

4.7. TENABLITY OF THE THOERETICAL MODEL

Explicit knowledge was provided to end-users in the form of the security awareness film. This knowledge was also made implicit by the fact that the end-users were required to write a security test. This implicit knowledge was measured and it was found that the training material must have been internalised since those end-users who had undergone training obtained higher test scores than those who had not undergone training. In that sense the impact of information security training was effective. However, based on the data at hand the subsequent requisite compliant security behaviour was not apparent. Since the theoretical model proposed in chapter 1 was based on the hypotheses presented in the previous sections it may be concluded that the model is partially supported by the data generated by this research. However, based on the existing data, internalised knowledge of security requirements is not sufficient to influence the required behaviours. This has implications for the existing literature as will be discussed in the next section of this chapter. Further studies should be conducted in order to verify the external validity of these results.

4.8. LITERATURE IMPLICATIONS

This research modifies the previous conclusions reached by researchers such as McCoy and Fowler (2004:349) and Sommers & Robinson (2004:379) who all experienced difficulties in measuring the effectiveness of their security awareness interventions and, consequently, did not carry out such measurements. This research has shown that measuring effectiveness of security awareness training is plausible and does provide valuable results.

In addition, based on the data of this research, the outcome may not always be expected and this, in one sense, supports some of the conclusions reached by Anandpara et al. (2007). Anandpara et al showed that, even when users underwent security education on phishing, the results did not indicate an improvement in the ability of the participants to identify phishing scams. All that actually happened was that the participants became more suspicious. So, in this respect, the research of Anandpara and colleagues is confirmed (2007). This research also supports their research which concluded that obtaining a high test score does not necessarily mean an improved ability to identify a phishing scam. This research also extends their research since, in this research, actual behaviour is measured and, therefore, this study is not burdened with the subject-expectancy effect.

In addition, the work of Furnell (2005) and Srikwan and Jakobsson, (2007) regarding the necessity of end-users understanding the underlying threat when it comes to awareness and the lack of effectiveness of (online) education is both supported and extended. Hypothesis 2 revealed that the training administered had been effective and that end-user feedback had been overwhelmingly positive.

On one level this research modifies the previous conclusions of writers and practitioners who believed that it is futile to educate users (Ranum, 2005; Evers, 2006; Nielsen, 2004). Based on this research it is clear that this view is rather too simplistic. This research has demonstrated that end-users did show an improved understanding of security and compliant behaviour was demonstrated. However, compliant behaviour has not been linked solely to the outcome of awareness training. The results of this research suggest that, while awareness is necessary, it is not sufficient to ensure compliance on the part of end-users. The data also suggests that security tests carried out by end-users may also have a moderating effect on their behaviour. Utterances by the aforementioned researchers are not helpful and confuse the nature of the problem even further. In this regard it would be more helpful to pose questions such as under what circumstances is it futile to educate users? Further evidence that awareness training is but one intervention necessary for compliance is provided by Straub & Welke (199:19). They state that the dissemination of security material, as well as publicly advertised efforts to detect non-compliant behaviour, will significantly deter such behaviour.

Ultimately, the answer may be to turn to the social theories and to look at aspects such as attitudes which affect intentions and which, ultimately, affect behaviour (Lee & Lee, 2002:60). The results of this research supports the importance of the behavioural aspects that have been called for previously by researchers such as Schultz, 2004:1, Siponen, 2001:24, Srikwan and Jakobsson, 2007:2 and Van Niekerk and von Solms, 2004.

Perhaps the greatest contribution of this research is its support of previous writers in the field of Behavioural Information Security. This field looks at the motivations behind security related behaviours. At face value the results support further exploration of the work of Kruger and Kearney (2005) who maintain that behaviour is determined by affect (a person’s emotions), behaviour (intention to act in a certain manner) and cognition (beliefs in respect of a certain issue). Pahnila et al. (2007) maintain that the promoting of positive social pressure supports actual compliance with policies. They are of the opinion that this should be accomplished by stating explicitly what needs to be done. All these arguments may be regarded as contributing factors to increasing compliance with policies. It is also possible that other factors, such as the values and beliefs of individuals, may also interfere with end-user behaviour. Thus, despite the fact that an employee may have fully comprehended the policy the employee may not act as required if there is a conflict with his/her belief system (Schlienger & Teufel, 2003). In respect of to the health care community it has been argued that a security culture needs to be entrenched in order for the security to become effective. This would require, inter alia, strong commitment on the part of senior management and clear lines of accountability and responsibility (Gaunt, 2000:157; Kajava & Siponen, 1997; Mitnick & Simon, 2002:252). The problem is more complex than merely heightening the awareness of employees – ethical considerations, external factors and the way in which employees perceive the organisation may all play a role in influencing security complaint behaviour.

The outcome of this research also refutes the conclusions of Vroom and von Solms (2004:191) who assert that it is far too difficult a process to measure employee behaviour and that the process could be flawed. This research has shown that, although the process may be complex, it is, nevertheless, possible and may also be automated to a large degree. The research has uncovered a wealth of information which would merit future analysis and also further work on developing a reliable measurement framework based on previous studies. This study is undoubtedly plausible.

Finally, this research also supports and extends the conclusions of Stanton et al. (2005). As in this study their conclusions demonstrate that the sharing of one's password (categorised as Naïve Mistakes) was not associated with training and awareness. Further conclusions by Stanton et al. (2005) found that the choice of strong passwords (Basic Hygiene) was associated with awareness and training. However this finding was not corroborated by this research. It must also be borne in mind that Stanton et al. (2005) used a national survey for their study whereas this research used direct-observation in a case study in which actual user behaviour was measured. It is, therefore, obvious that this study extended the conclusions and research of Stanton et al. (2005).

4.9. SUMMARY

This chapter presents the results of the research strategies implemented in respect of each hypothesis. The results were presented in terms of sampling, data collection and data analysis. It would appear that security awareness intervention alone does not significantly influence security behaviours as measured in terms of Naïve Mistakes, Detrimental Misuse and Basic Hygiene. Although dramatic improvements were noted after the awareness training these improvements were observed in both groups (most notably in Basic Hygiene) and could, therefore, not be attributed to training alone. It would seem that the completing of the security tests was a factor in influencing subsequent compliant behaviour by possibly triggering prior learning. The security awareness training was effective in terms of internalised knowledge as the experimental group scored significantly better than the control group. Finally, it was shown in this study that undergoing training and achieving high scores in the security tests were not associated with compliant behaviour.

The results of this study were, thus, referenced to prior research studies and areas in which these results support, extend and refute existing research. Further research in the field of Behavioural Information Security is strongly advocated.

CHAPTER 5 : CONCLUSION

And those who were seen dancing were thought to be insane by those who could not hear the music.

Friedrich Nietzsche (Quote DB, 2008)

5.1. OVERVIEW OF THE STUDY

There are two major contributions made by this research report. Firstly, it was shown that there is a dearth of in-depth information and security awareness research and that behavioural concepts are not properly taken into account in security awareness programmes. There is also a lack of theoretical models which explain the way in which awareness training affects behaviour. This study built on existing behavioural information security research and proposes a theoretical model which is based on an organisational learning model.

Secondly, this research tested the proposed model empirically by using system-generated data as indicators of behaviour in a pretest-posttest experimental design. Therefore no reliance was placed on the perceptions of users in respect of their own behaviour. Previous research has used interviews, surveys and "participatory observation" in order to draw conclusions about end-user behaviours in this regard. This study measured the subset of behaviours required by a typical AUP whereas much of the previous and recent research in respect of training effectiveness has focused on phishing related threats. The objective of this research was to determine the effectiveness of the information security awareness training that was administered to end-users. The research produced a set of instruments that could be used for behavioural measurement in future research. It is these preceding factors which the researcher believes sets this research apart from the existing literature and contributes to the resolution of the research problem. The outcome of this research could help researchers and practitioners understand the reasons why an awareness initiative is expected to produce certain results in respect of security behaviour and, consequently, this model would provide practitioners with practical guidance in terms of their information security programmes.

5.2. SUMMARY OF THE RESULTS

The results of this research found that the security awareness training was effective in terms of the end-users in question retaining more security knowledge than those end-users who had not undergone security awareness training. However, there was no evidence to suggest that security awareness alone is sufficient to ensure compliant behaviour by end-users. Although dramatic improvements were noted after the awareness training these improvements were seen in both groups (most notably for Basic Hygiene) and could, therefore, not be attributed to training alone. It would appear that completing the security tests was a factor in influencing subsequent compliant behaviour by possibly triggering prior learning. It is further maintained that security awareness training is a necessary, integral component that may influence compliant behaviour but is not adequate to do so fully. Practitioners must insist that their security awareness programmes are measured in terms of effectiveness and that these programmes should focus on behavioural aspects in order to complement awareness initiatives. Finally, this study showed that undergoing training and achieving high scores in the security tests were not associated with compliant behaviour.

Table 30 explains the outcomes of the hypothesis testing.

Table 30: Hypothesis testing outcome

Hypothesis #	**Explanation**	**Verdict**
H1	This hypothesis tested the impact of security awareness training on three security behaviours. Improvements were noted in both groups but these were not attributed solely to training.	Not Supported
H2	This hypothesis test end-users' comprehension of the policy. The group that underwent the training achieved a significantly better test score than those that had not undergone training.	Supported
H3	End-users who underwent training and subsequently exhibited non-compliant behaviour did not score significantly lower on the security test than those who were compliant.	Not Supported

5.3. RECOMMENDATIONS AND IMPLICATIONS

5.3.1. Recommendations for further study

Security awareness training should influence all employees within an organisation to ensure the appropriate behaviour is enacted by all and, in this way, bring about compliance with information security policies. In order to confirm this statement the following questions should be further explored: In terms of explicit knowledge what type of security awareness training would be more likely to influence behaviour i.e. how important is the quality of the awareness material and the mechanism of delivery? What role do security tests play in refreshing the prior security knowledge of users? In what ways could practitioners deliver the awareness message more effectively in order to ensure greater participation on the part of end-users? This research employed a novel way in which to distribute the awareness material to end-user desktops. Standardised, cost-effective and automated mechanisms for gathering system generated data (especially for those behaviours which require high levels of expertise) and the feasibility of such mechanisms merit additional investigation. This research has demonstrated that it is possible to automate security behaviour measurement by using standard techniques and tools. In terms of implicit knowledge further standardised mechanisms should be explored to determine how best to measure implicit knowledge whilst also taking into account the role of principles of the learning sciences. What are the most effective learning principles and under what conditions are they effective? It is also important that future research determine the status of employees within the organisation and the role played by this in awareness training. Once users have fully comprehended policies are the same types of interventions necessary in order to sustain the required behaviours? This is important as it would probably determine the frequency of future awareness interventions. Longitudinal studies in this regard would be necessary. Longitudinal studies are also needed in order to determine the impact of behaviour over the long term. An understanding of the influence of factors such as user attitude, perceptions and corporate politics on the internalisation of the security awareness message and subsequent behaviour is also essential. Finally, further research is needed on a taxonomy of security behaviours. Such research would further build on the work of Stanton et al. (2005).

5.3.2. Recommendation and Implications for the Industry

According to Dhillon (1999) increasing the awareness of security issues is the most cost-effective control that may be implemented by an organisation. Research that contributes to the effectiveness of awareness would ultimately benefit organisations as a whole as such research would allow organisations to focus on techniques that would improve the intentions of their employees and ultimately enhance end-user security behaviours. The literature survey in chapter 2 strongly implies that further research is needed in this respect. Diverse methods to be used in the measuring of different behaviours are also called for (Stanton et al., 2005) and this need has been highlighted by this research. This research also contributes to a standard set of instruments that could be useful to practitioners in the future. The techniques used in this report to measure security behaviours could be expanded to include a basket of security behaviours. The instruments used are more suitable to measuring behaviour which requires low technical expertise and measurements of malicious types of behaviour would not be as easy to obtain (Stanton et al., 2005). Hence, in this respect, other methods would have to be used and there are commercial tools available for this. Nevertheless, these types of measurements could be presented to senior management as part of the monthly security report.

The implications for practitioners are potentially significant. In order for an organisation to implement effective information security it is essential to gain the understanding of all the employees within the organisation. In addition, compliance with security policies is necessary and, in some cases, this compliance needs to be demonstrated by either the information security function or the risk management function within an organisation in order to justify their activities. At face value the outcome of this research points to the fact that security awareness training, while important, is not sufficient to prevent non-compliant behaviour and to ensure compliant behaviour. Practitioners should, therefore, not rely on awareness alone if they wish the message to be both meaningful and effective. The literature survey points to many examples in terms of which reliance is placed on awareness alone. This research provides pragmatic guidance for practitioners when designing and implementing their information security awareness programmes.

The results of this research could also be financially beneficial to organisations since, if it is further corroborated that behavioural security aspects such as attitude, and positive reinforcement are key, then organisations could channel their resources into the most cost-effective methods. It is not cost effective to spend blindly on information security awareness campaigns without an appropriate mechanism to measure the effectiveness of these campaigns and whether a difference is made to actual behaviour. Therefore, it must be ascertained which techniques have the greatest impact on behaviour as this would result in the most effective techniques being used and inefficient techniques being avoided. The altering of the intentions of employees to become more positive would, ultimately, benefit organisations. Thus the outcomes of this research could enable organisations to focus on techniques that improve their employees' intentions and, ultimately, encourage more positive end user security behaviours. In addition, this research contributes a set of tools or techniques that future researchers and practitioners could use and improve in order to measure end-user behaviour.

5.4. RESEARCH LIMITATIONS

It is important to note that there are a number of extenuating circumstances and boundaries in terms of this research. Firstly, the instrument used to measure Detrimental Misuse could, in some respects, be considered a blunt tool as it also measured internal browsing, for example, browsing of the corporate Intranet as well as Internet browsing. In addition, this particular behavioural measurement did not distinguish between "good" browsing and "bad" browsing. For example, browsing Internet banking websites may be considered "good" browsing as opposed to online gaming which is considered a waste of company resources. The organisation's AUP allows for business-related and, even occasional personal, browsing. However, the policy is not prescriptive about limits and about what is acceptable. Email abuse by end-users was also not measured.

In terms of Basic Hygiene the passwords tested had already been subjected to password complexity rules. This means that the system had already screened the passwords chosen by users before the passwords were accepted by the system. Thus users could not simply enter *123* as a password. Enforced password complexity may, therefore, have played a role in minimising the differences between the control and the experimental group members since both groups would have had to enter passwords with at least a basic level of complexity. Note that password complexity rules do not guarantee that users will choose strong passwords. This is substantiated by the fact that prior to training it was possible to crack a total of 922 passwords with password complexity which had been enabled on the system.

Finally, translating the organisation's AUP into film format was challenging since there was a lot of material that had to be conveyed. Accordingly it was necessary to divide the film into three 15-minute parts and to screen these separate parts to users at separate times. Consequently user participation waned from the first to the third showing of the film (see chapter 4 for the response rates for each part of the film). Despite coupling the awareness to a competition and sending out reminder emails to end-users the response rate was lower than anticipated. Future research could couple this awareness training to the employee performance contract to ensure a high response rate.

5.5. CONCLUSION

The contribution of this research is significant in the following ways: The research comprised a case study that used system generated data to measure actual user behaviour both before and after the security awareness training intervention in order to determine the effectiveness of the training. For this reason no reliance was placed on the perceptions of the users about their own behaviour. Existing research has used interviews, surveys and "participatory observation" in order to draw conclusions about end-user behaviour in this regard. This research measured a subset of the behaviours required by a typical Acceptable Usage Policy, whereas much of the existing and even recent research with respect to awareness training effectiveness has focused on phishing related threats in a laboratory environment. This research not only demonstrated the impact of security awareness training on user behaviour but it also makes a contribution to devising a set of instruments that could be used in future research on behavioural measurement. This research aimed to consolidate the security awareness research landscape and to move towards a common understanding and language of the meaning of "security behaviour".

REFERENCES

Anandpara, V., Dingman, A., Jakobsson, M., Liu, D. & Roinestad, H. 2007. Phishing IQ tests measure fear, not ability. In *Usable security* (USEC'07). http://usablesecurity.org/papers/anandpara.pdf

Aytes, K. & Connolly, T. 2003. A research model for investigating human behavior related to computer security. Proceedings of the 2003 American Conference on Information Systems, Tampa, FL, August 4-6.

Banerjee, D., Cronan. T.P. & Jones, T.W. 1998. Modeling IT ethics: A study in situational ethics. *MIS Quarterly*, 22(1), pp 31–60.

Barman, S. 2002. *Writing IS security policies*. Indianapolis: New Riders Publishing.

Baskerville, R. 1999. Investigating information systems with action research. *Communications of the Association for Information Systems,* Vol. 2, pp 2–30.

Baskerville, R. & Wood-Harper, T. 1996. A critical perspective on action research as a method for information systems research. *Journal of Information Technology* Vol. 11, pp 235–246.

Beatson, J.G. 1991. Security - a personnel issue. The importance of personnel attitudes and security education. Proceedings of the Sixth IFIP International Conference on Computer Security.

Bray, T.J. 2002. Security actions during reduction in workforce efforts: What to do when downsizing. *Information System Security*, 11(1), pp 11–15.

Paypal. 2008 [online]. [Accessed 2008]. Available from World Wide Web: <https://www.paypal.com/fightphishing >

Computer Security Institute (CSI). 2006. *Virus attacks named leading culprit of financial loss by US companies in 2006 CSI/FBI Computer Crime and Security Survey* [online]. [Accessed 9th August 2006]. Available from World Wide Web: http://www.gocsi.com/press/20060712.jhtml

Computer Security Institute (CSI). 2007. *The 12th Annual Computer Crime and Security Survey* [online]. [Accessed: 2007]. Available from World Wide Web: http://www.gocsi.com/forms/csi_survey.jhtml

Cox, A., Connolly, S. & Currall, J. 2001. Raising IS security awareness in the academic setting. *VINE*, Issue 123, pp 11–16.

Dark Reading, 2007.
http://www.darkreading.com/blog.asp?blog_sectionid=447&doc_id=132244

Deloitte 2006. *Global Security Survey*:
http://www.deloitte.com/dtt/cda/doc/content/us_fsi_150606globalsecuritysurvey(1).pdf

Denning, D.E. 1999. *Information warfare and security*. USA: ACM Press.

Desman, M.B. 2002. *Building an IS security awareness program* USA: Auerbach Publications.

Detmar, W., Straub, Jr & Nance, W.D. 1990. Discovering and disciplining computer abuse in organisations: A field study. *MIS Quarterly*, 14(1), pp 45–60.

Dhillon, G. 1999. Managing and controlling computer misuse. *Information Management & Computer Security*, 7(4), pp 171–175.

Drucker P.F. 1993. *Post-capitalist society*. Oxford: Butterworth Heinemann.

Eloff, M.M. & von Solms, S.H. 2000a. Information security management: A hierarchical framework for various approaches. *Computers & Security*, Vol. 19, pp 243–256.

Eloff, M. & von Solms, B. 2000b. Information security: Process evaluation and product evaluation. In: *Information security for global information infrastructures*. IFIP TC11 Sixteenth Annual Working Conference on Information Security. Norwell, MA, USA: Kluwer Academic Publishers, pp 11–18. Conference Paper.

Evers, J. 2006. *Security expert: User education is pointless* [online]. [Accessed 2007]. Available from World Wide Web: <http://www.news.com/Security-expert-User-education-is-pointless/2100-7350_3-6125213.html?tag=item>

Finne T. Information Systems Risk Management: Key Concepts and Business Processes. *Computers & Security*, Vol. 19, 2000, pp 234–242.

Federal Bureau of Investigation (FBI) – Minneapolis Field Division. 2008. [online]. [Accessed 9 February 2008]. Available from World Wide Web: http://minneapolis.fbi.gov/dojpressrel/pressrel08/logicbomb011008.htm

FCW. 2001 [online]. [Accessed 2007]. Available from World Wide Web: http://www.fcw.com/print/7_17/news/73778-1.html

Ferguson, A.J. 2005. Fostering e-mail security awareness: The West Point Carronade. *EDUCASE Quarterly*. 1. Retrieved March 22, 2006, http://www.educause.edu/ir/library/pdf/eqm0517.pdf, pp 54–57

Forcht, K.A., Pierson, J.K. & Bauman, B.M. 1988. Developing awareness of computer ethics. Proceedings of the ACM SIGCPR conference on management of information systems personnel, pp 142–143.

Furnell, S., Sanders, P.W. & Warren, M.J. 1997. Addressing IS security training and awareness within the European healthcare community. In Proceedings of Medical Informatics Europe '97.

Furnell, S.M., Gennatou, M. & Dowland, P.S. 2000. Promoting security awareness and training within small organizations. Proceedings of the First Australian Information Security Management Workshop, Geelong, Australia.

Furnell, S.M., Gennatou, M. & Dowland, P.S. 2002. A prototype tool for IS security awareness and training. *International Journal of Logistics Information Management*, 15(5), pp 352–357.

Furnell, S.M. 2005. Why users cannot use security. *Computers & Security,* 24(4), pp 274–279.

General Accounting Office (GAO). 1998. *Information security management: Learning from leading organisations*. http://www.gao.gov/special.pubs/ai9868.pdf (2002), United States of America, General Accounting Office.

Government Accountability Office (GAO). 2005. *Information security continued efforts needed to sustain progress in implementing statutory requirements*. http://www.gao.gov/new.items/d05483t.pdf (2005), United States Government Accountability Office.

Gaunt N. 2000. Practical approaches to creating a security culture. *International Journal Of Medical Informatics*, 60(2), pp 151–157.

Gaunt, N. 1998. Installing an appropriate IS security policy in hospitals. *International Journal of Medical Informatics*, pp 131–134.

Hansche, S., Berti, J. & Hare, C. 2004. *Official (ISC)^2 guide to the CISSP exam* New York: Auerbach Publications.

Information Security Forum (ISF). 2005. *The standard of good practice*. London. Information Security Forum.

Jagatic, T.N., Johnson, M., Jakobsson, M. & Menczer, F. 2007. Social phishing. *Communications of the ACM*, 50(10), pp. 96–100.

Janczewski, L. & Xinli Shi, F. 2002. Development of information security baselines for healthcare information systems in New Zealand. *Computers & Security,* 21(2), pp 172–192.

Johnston, J., Eloff, JHP. & Labuschagne, L. 2003. Security and human computer interfaces. *Computers & Security,* 22(8), December, pp 675–684.

Kabay, M.E. 2002. Using Social psychology to implement security policies In: Bosworth, S. & Kabay, M.E. (eds) *Computer security handbook* (4th edition). USA: John Wiley & Sons.

Kajava, J. & Siponen, M.T. 1997. Effectively implemented IS security awareness: An example from university environment. Proceedings of IFIP-TC 11 (Sec'97/WG 11.1), 13th International Conference on IS security: IS security Management - The Future.

Katsikas, S.K. 2000. Health care management and information systems security: Awareness, training or education? *International Journal of Medical Informatics*, Vol. 60, pp 129–135.

Keeney, R.L. 1996. Value-focused thinking: Identifying decision opportunities and creating alternatives. *European Journal of Operational Research*, 92(3), pp 537–549.

Kluge, E.H.W. 1998. Fostering a security culture: A model code of ethics for health information professionals. *International Journal of Medical Informatics* 49(1), pp 105–110.

Kovacich, G.L. 1998. *Information system security officer's guide: Establishing and managing an information protection program*. USA: Butterworth-Heinemann.

Kovacich, G.L. & Halibozek, E.P. 2003. *The manager's handbook for corporate security: Establishing and Managing a successful assets protection program.* USA: Butterworth-Heinemann.

Kruger, H.A., Drevin, L. & Steyn T. 2006. A framework for evaluating ICT security awareness. Proceedings of the ISSA 2006 from Insight to

Foresight Conference 5 July – 7 July, Balalaika Hotel, Sandton, South Africa.

Kruger, H.A. & Kearney, W.D. 2005. Measuring information security awareness: A West Africa Gold Mining environment case study. Peer-reviewed Proceedings of the ISSA 2005 New Knowledge Today Conference 29 June – 1 July, Balalaika Hotel, Sandton, South Africa.

Kumaraguru, P., Sheng, S., Acquisti A., Cranor, LF. & Hong J. 2007a *Teaching Johnny not to fall for phish*. CMU Technical Report, February 8,

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J. & Nunge, E. 2007b. Protecting people from phishing: The design and evaluation of an embedded training email system. Conference on Human Factors in Computing Systems archive. Proceedings of the SIGCHI conference on Human factors in computing systems. San Jose, California, USA, , pp. 905 – 914.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. & Hong, J. 2007c. Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. ACM International Conference Proceeding Series, Vol. 269, Proceedings of the anti-phishing working groups, 2nd annual eCrime researchers summit, Pittsburgh, Pennsylvania. pp. 70 – 81,

Lafleur, L.M. 1992. Training as part of a security awareness programme. *Computer Control Quarterly*, 10(4), pp 4–11.

Leach J. 2003. Improving user security behaviour. *Computers & Security*, 22(8), pp 685–692.

Lee, J. & Lee, Y. 2002. A holistic model of computer abuse within organizations. *Information Management & Computer Security*, 10(2), pp 57–63.

Madigan, E.M., Petrulich, C. & Motuk, K. 2004. The cost of non-compliance: When policies fail. Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services, Baltimore, MD, USA: ACM Press. New York, NY, USA, pp 47–51.

Markey, E. 1989. Getting organizations involved in computer security: The role of security awareness. Proceedings of the Fifth IFIP International Conference.

Martins, A. & Eloff, J.H.P. 2002. IS security culture. Proceedings of IFIP TC-11 17th International Conference on IS security (SEC2002).

McCoy, C. & Fowler, R.T. 2004. You are the key to security: Establishing a successful security awareness program. Proceedings of the 32nd annual ACM SIGUCCS conference on User services, Baltimore, Maryland, pp 346-349.

Mende, J. 2006. *Chapter 3 - Research Methods,* lecture notes distributed in the topic module code Research Reporting. University of the Witwatersrand, Johannesburg on 6 December.

Methods of Conceptual Analysis. [online]. [Accessed 9 May 2008]. Available from World Wide Web: <http://writing.colostate.edu/guides/research/content/pop3a.cfm>

Mitnick, K.D. & Simon, W.L. 2002. *The art of deception: Controlling the human element of security.* USA: John Wiley & Sons.

Murray B. 1991. Running corporate and national security awareness programmes. Proceedings of the IFIP TC11 Seventh International Conference on IS security, pp 203–207.

NIST. 1998. Information Technology Security Training Requirements: A Role- and Performance-Based Model. *NIST Special Publication 800-16.* U.S. Government Printing Office, Washington.

Neumann, P.G. 2003. Information systems security redux. *Communications of the ACM*, 46(10), pp 136.

Nielsen, J. 2004. *User education is not the answer to security problems* [online]. Accessed [Accessed: 2007]. Available from World Wide Web: <http://www.useit.com/alertbox/20041025.html>

Nonaka, I. & Takeuchi, H. 1995. *The knowledge creating company*. New York: Oxford University Press.

Nosworthy, J.D. 2000. Implementing information security in the 21st century: Do you have the balancing factors? *Computers & Security*, Vol. 19, pp 337–347.

OECD. 2002. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* [online]. [Accessed: 2006]. Available from World Wide Web: <http://www.oecd.org/dataoecd/16/22/15582260.pdf>

Pahnila, S., Siponen, M. & Mahmood, A. 2007. Employees’ behavior towards IS security policy compliance. Proceedings of the 40th Hawaii International Conference on System Sciences,

Pallant, J. 2001. *SPSS survival manual.* Philadelphia: Open University Press.

Parker, D.B. 1998. *Fighting computer crime: A new framework for protecting information*. USA: John Wiley & Sons.

Perry, W.E. (1985). *Management strategies for computer security*. USA: Butterworth.

Peltier, T. 2000. How to build a comprehensive security awareness program. *Computer Security Journal*, 16(2), pp 23–32.

Puhakainen, P. 2006. A design theory for information security awareness. Ph.D. thesis, University of Oulu.

Quote DB. [online]. [Accessed 17th August 2008]. Available from World Wide Web: < http://www.quotedb.com/quotes/4132>

Ranum, M. 2005. *The six dumbest ideas in computer security* [online]. [Accessed: 2007]. Available from World Wide Web: <http://www.ranum.com/security/computer_security/editorials/dumb/>

Robila, S.A. & Ragucci, J.W. 2006. Don't be a phish: Steps in user education. ITICSE '06: Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education, New York, NY, USA, pp 237-241.

SABS ISO/IEC 17799 (SABS). 2000. *Information technology: Code of practice for information security management.* Pretoria: South African Bureau of Standards.

SANS Institute. 2006a. *SANS NewsBites, Volume VIII, Issue 69.* 1 September 2006. [online]. [Accessed 2006]/ Available from World Wide Web: <http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=69#sID06>

SANS Institute 2006b. *SANS NewsBites, Volume VIII, Issue 70.* 5th

September [online]. [Accessed 2006]. Available from World Wide Web: <http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=70#sID301>

SANS Institute, 2006c. *SANS NewsBites, Volume VIII, Issue 71.* 8th September. [online]. [Accessed 2006]. Available from World Wide Web: <http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=71#sID201>

Schlienger, T. & Teufel, S. 2002. IS security culture: The socio-cultural dimension in is security management. Proceedings of IFIP TC 11.

Schlienger, T. & Teufel, S. 2003. Information security culture: From analysis to change. Proceedings of the 3rd Annual Information Security South Africa Conference, 9-11 July, Sandton, South Africa, pp. 183–196.

Schlienger, T. & Teufel, S. 2005. Tool supported management of information security culture: An application to a private bank. In: R. Sasaki, E. Okamoto & H. Yoshiura (Eds). The 20th IFIP International Information Security Conference (SEC 2005) – Security and Privacy in the age of ubiquitous Computing, Makuhari Messe, Chiba, Japan, Kluwer Academic Press.

Schneier, B. 2000. *Secrets & lies*. New York: Wiley Computer Publishing.

Schneier, B. 2003. *Beyond fear*. New York: Copernicus Books.

Schneier B. 2006. Educating users. August. *Schneier on Security BLOG.* [online]. [Accessed 26th August 2006]. Available from World Wide Web: <http://www.schneier.com/blog/archives/2006/08/educating_users.htm>

Schultz, E. 2004. Security training and awareness: Fitting a square peg in a round hole. *Computers & Security*, 23(1), pp 1–2.

Siponen, M.T. 2001. Five dimensions of information security awareness. *Computers and Society*, 32(2), pp 24–29.

Siponen, M.T. 2000a. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), pp. 31–41.

Siponen, M.T. 2000b. On the role of human morality in information system security: The problems of descriptivism and non-descriptive foundations. Proceedings of IS security for Global Information Infrastructures, IFIP TC11 Fifteenth Annual Working Conference on IS security, pp 401-410.

SonicWALL. Phishing and SPAM IQ Quiz by SonicWALL. [online]. [Accessed 14th February 2008]. Available from World Wide Web: <http://www.sonicwall.com/phishing>

Sommers, K. & Robinson, B. 2004. Security awareness training for students at Virginia Commonwealth University. In the proceedings of the SIGUCCS'04, Baltimore, Maryland, October 10-13, pp 379–380.

Spurling, P. 1995. Promoting security awareness and commitment. *Information Management & Computer Security*, 3(2), pp 20–26.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti A., Cranor, LF., Hong, J. & Nunge, E. 2007. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. ACM International Conference Proceeding Series; Vol. 229, Proceedings of the 3rd symposium on Usable Privacy and Security, pp 88–99.

Srikwan, S. & Jakobsson, M. 2007. *Using cartoons to teach Internet Security* [online]. [Accessed 2007]. Available from World Wide Web: <http://www.informatics.indiana.edu/markus/documents/security-education.pdf>

Stanton, J.M., Stam, K.R., Guzman, I. & Caldera, C. 2003. Examining the linkage between organizational commitment and information security. *Proceedings of the IEEE Systems, Man, and Cybernetics Conference.* Washington, DC.

Stanton J.M., Stam, K.R., Mastrangelo, P., Jolton, J. 2005. Analysis of end user security behaviours. *Computers & Security,* Vol. 24, pp 124–133.

Stanton, J.M. & Stam, K.R. 2006. *The visible employee.* New Jersey: Information Today.

Stephanou, A.T. & Dagada, R. 2008. The impact of information security awareness training on information security behaviour: The case for further research. Proceedings of the ISSA 2008 Innovative Minds Conference, 7 – 9 July, School of Tourism & Hospitality, University of Johannesburg, South Africa.

Straub, D.W. 1990. Effective IS security: An empirical study. *Information Systems Research* 1(3), pp 255–276.

Straub, D.W., Carlson, P.J. & Jones, E.H. 1993. Deterring cheating by student programmers: A field experiment in computer security. *Journal of Management Systems*, 5(1), pp 33–48.

Straub, W. & Welke, R.J. 1998. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4), pp 441–469.

Thomson, M.E. & von Solms, R. 1998. Information security awareness: Educating your users effectively. *Information Management & Computer Security,* 6(4), pp 167–173.

Trompeter, C.M. & Eloff, J.H.P. 2001. A framework for the implementation of socio-ethical controls in information security. *Computers & Security*, Vol. 20, pp 384–391.

Van Niekerk, J. & von Solms R. 2004. Organisational learning models for information security. Peer-reviewed Proceedings of the ISSA 2004 enabling tomorrow conference 30 June – 2 July, Gallagher Estate, Midrand.

Von Solms, B. 2000. Information security: The third wave. *Computers & Security*, Vol. 19, pp 615–620.

Vroom, C. & von Solms, R. 2004. Towards information security behavioural compliance. *Computers & Security*, Vol. 23, pp 191–198.

Vyskoc, J. & Fibikova, L. 2001. IT users' perception of IS security. Proceedings of the IFIP WG 9.6/11.7 Working-Conference.

Welman, J.C. & Kruger, S.J. 2001. *Research methodology*. New York: Oxford University Press.

Woon, I.M.Y., Tan, G.W. & Low, R.T. 2005. A protection motivation theory approach to home wireless security, Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas, pp 367–380.

Whalen, T. & Inkpen, K.M. 2005. Gathering evidence: Use of visual security cues in web browsers. ACM International Conference Proceeding Series, Vol. 112. In Proceedings of the 2005 Conference on Graphics interface, Victoria, British Columbia, May 09–11, pp. 137–144.

APPENDIX A – ACCEPTABLE USAGE POLICY (AUP)

The following text is an extract from the Acceptable Usage Policy of the organisation in question.

INTRODUCTION

This Acceptable Usage Policy shall be deemed to have been accepted by the User (being the Employee or a Trading Partner) on commencement of the employment relationship or business relationship, as the case may be.

Information is an asset that the organisation heavily relies on to conduct its daily business, to make informed business decisions and to achieve its vision and business goals. To support the effective usage of these Information Assets, IT Systems have been installed as key business tools.

This policy guides the usage and maintenance of the organisation's information and the supporting equipment and Systems to assist with:

- The completion of all business processes within reasonable time;
- Business decisions being based on reliable and up to date information;
- The achievement of cost savings through the optimal usage of the resources.

Abuse of the organisation's IT Systems can have far-reaching repercussions such as exposure to risks, compromise of Systems and services and legal issues and is therefore seen as a serious offence. Any breach of these regulations will result in disciplinary action being taken against offenders, in accordance with the organisation's disciplinary procedures. The aim of this policy is not to impose restrictions that are contrary to TOPAZ CC's established culture of openness, trust and integrity, but rather to ensure that the organisation is adequately protected from illegal or damaging actions by Individuals, either knowingly or unknowingly.

COMPLIANCE, MONITORING AND AUDITING

Failure to comply with this policy or any of the supporting and complimenting policies, standards and / or processes will result in a security violation and the appropriate disciplinary action being taken. The appendices form part of this policy and must be read in conjunction with the document.

TOPAZ CC reserves the right to intercept and/or monitor all communications and/or the use of all IT Systems and services, including (without limitation) e-mail and Internet usage, for security, management and maintenance purposes and any other lawful purpose. Workstations may be regularly audited to confirm compliance to the acceptable use of the equipment. Should inappropriate content or use be identified, disciplinary action may be taken in accordance with the organisation's official disciplinary procedures. Interception and/or Monitoring activities may take place without prior notification if deemed necessary.

EXCEPTION HANDLING

All exceptions to this Acceptable Usage Policy will be fully motivated and documented by those seeking an exception to the policy, and agreed to by the relevant affected parties. All exceptions will be reviewed at least annually by the relevant Individual/s tasked with risk management around the particular area/s affected by the exception.

GENERAL USE AND OWNERSHIP

The workstation(s), other IT Systems, and access to the organisation's IT Systems and information are provided to you to enable you to fulfil your daily function in the organisation. It is therefore expected of you to:

1. Use the Systems primarily for organisational business purposes, with good judgement exercised regarding the reasonableness of personal use;
2. Use the access and information solely for organisational business purposes, whilst striving to maintain the privacy and confidentiality thereof as per the organisation's non-disclosure and confidentiality agreements;
3. Use the IT Systems as set up, without attempting to change the security settings and configuration, including the hardware;
4. Take note that all information created on or stored on the organisation's Systems is the property of TOPAZ CC, regardless whether originally created for personal or organisational use and its confidentiality therefore cannot be guaranteed. For instance, when leaving the organisation's employ or during suspension you may therefore not delete or copy any work-related information, including e-mail;
5. Not abuse the organisation's IT resources or those of any other organisation you utilise in the course of your daily operations;
6. Adhere to good risk management practices, such as clean desks and secure laptop usage;
7. Not connect any devices, whether internal or external, to the provided IT System, unless authorised;
8. Not connect IT Systems, including workstations and laptops, not owned by TOPAZ CC to the TOPAZ CC production environment, unless authorised by IS;
9. Not create or connect to any domains other than the official TOPAZ CC production environment domains;
10. Not make your workstation available for remote use and/or management, unless specifically authorised.

LOGICAL ACCESS CONTROL

Your user ID and password are the key defences for the organisation's equipment, Systems and information. To protect these, you are expected:

1. Not to allow other Users to use your user ID as you will be held responsible for all activities performed with it;
2. To use well chosen passwords and change them regularly, as prompted by the various Systems. Where possible, ensure that the password consists of mixed case, numerical characters and special characters and avoid the use of personal information and dictionary words in the password;
3. Not to share your password with anyone, including IT support staff, nor to keep a record of it in an obvious place;
4. Not to use any other User's user ID and password;
5. To take corrective steps, should you suspect that your user ID and password have in any way been compromised;
6. Not to request any password to be reset, other than your own, nor to attempt to guess other Users' passwords. Managers may request the reset of passwords on behalf of their Employees, provided that proof of the request from the Employee can be provided upon demand;
7. Not to select the option to remember your password when logging on to applications, services and network links, including the Internet;
8. To use the Windows lock mechanism (**CTRL** + **ALT** + **DEL** to activate) or terminate active application sessions when leaving your workstation unattended for an extended period of time;
9. Not to access information resources not within the scope of your work. The principle of least privilege access will be applied;
10. To respect the access assigned to you and not to abuse your legal access or any privileged access, such as provided to administrators for monitoring purposes.

MALICIOUS CODE / VIRUS PROTECTION

The organisation's information is vulnerable to attack from viruses and other malicious code. Although technical solutions have been implemented to mitigate the risks posed by viruses, the speed with which these are developed and spread requires that every User additionally takes certain actions to minimise the risks. These are as follows:

1. Respond immediately to any viruses or malicious code the anti-malicious code software detects on your workstation by informing the IS Command Centre. The IS Command Centre will assist in identifying and removing the malicious code and repairing any damage that resulted from the

malicious code infection;

2. Do not de-install, deactivate, reconfigure or attempt to circumvent the anti-malicious code software installed on your workstation;
3. Do not attempt to bypass the automated logon scripts aimed at updating the anti-malicious code software and virus definitions / signature files and operating system patches;
4. Do not open suspicious e-mail attachments even if they are from known and trusted sources;
5. Do not execute programmes received by e-mail until it has been determined that the programmes are from a trusted source;
6. Do not download software from an unknown and untrusted source. Only use software obtained from IS. Only authorised Individuals may download software for test purposes in controlled environments;
7. Do not knowingly get involved in any action that would lead to the creation or distribution of viruses or other malicious code;
8. Ignore all pop-up windows appearing on screen when browsing the Internet, as these may contain Spyware, which is defined as any software that covertly gathers information about a User while he / she is navigating the Internet and then transmits the information to an Individual or organisation that uses it for marketing or other purposes;
9. Do not forward or create any virus notifications or hoax messages. All communication regarding viruses or other malicious code will be done via official communication channels;
10. Do not use any IT System unless IS has authorised and confirmed to you that it has scrutinised and verified the IT Systems and anti-malicious code installations of third parties reporting to you that need to connect to the TOPAZ CC network.

MOBILE COMPUTING

When using mobile computing devices, including but not limited to laptops, notebooks, PDAs and mobile phones, special care should be taken to ensure that the organisational information stored thereon is not compromised. Therefore, the following applies:

1. IS support will only be provided for approved mobile computing device models and brand names;
2. Personally owned mobile computing devices will only be allowed connectivity to the environment after approval and scrutiny from IS;
3. Secure settings will be implemented by IS on all mobile computing devices taking into consideration the limitations of the individual devices. These may not be circumvented;
4. Extra care should be taken when using mobile computing devices in public places, meeting rooms and other unprotected areas outside the

organisation's premises to avoid the risk of accidental or deliberate information gathering by unauthorised parties and to protect the device from theft or destruction.

SOFTWARE USAGE

The workstation(s) and other IT Systems provided to you are supplied with all the software that you need for work purposes. All software needed to maintain and keep track of the IT System has also been installed on it and may not be tampered with. IS will not support any non-standard configurations and reserves the right to remove these from the network should they pose a security risk to the organisation. To ensure that the software continues to fulfil its intended purpose, you are expected to:

1. Not under any circumstances install or download any unauthorised or unlicensed software, including games;
2. Not take it upon yourself to install patches and service packs, except when clearly instructed by the IS Command Centre. An automated function will ensure that your workstation is adequately protected as required by the organisation;
3. Contact the IS Command Centre if you need additional software as they will ensure that your request is dealt with via the correct procedures and that only properly authorised and licensed software is installed;
4. Procure all software via the IS Management Services and related procurement processes.
5. The retrieval of executable files, including freeware or shareware is strictly prohibited, unless for business purposes.

INTERNET USAGE

The Internet can be a valuable source of information, but at the same time poses serious risks to the organisation's information, Systems and network resources. Therefore, it is important to take note of the following:

1. Access to the Internet will be granted by management for business-related purposes only to further the interests of the organisation and its clients and customers. Acceptable use includes the downloading of software upgrades and patches by IT support, review of possible vendor sites for product information, reference of regulatory or technical information and research. It should not be used for private business activities, amusement or entertainment purposes. Occasional personal use of the Internet is permitted at the discretion of your manager and/or the Chief Information Officer (CIO), which is a privilege that should not be abused. Follow the corporate principles regarding resource usage and exercise good judgement when using the Internet;

2. Internet usage is recorded and reported on. If you are using the service inappropriately you may find yourself subject to disciplinary action;
3. Never install additional Internet access software such as a separate ISP connection. All Internet access must be provided through the corporate System;
4. Refrain from accessing non-business related webcams, video clips, audio files, automated downloads, streaming programmes or polling programmes via the Internet, as they cause unnecessary congestion on the network;
5. Subscriptions to chat rooms or instant messaging services requires the authorisation of your line manager and will be relevant to your job and industry. Social chatting is not allowed.
6. Where information from the Internet is used for TOPAZ CC business decisions, the integrity and the source of the information must be verified. Additionally, care must be taken not to violate any copyright laws when using information obtained from the Internet

E-MAIL USAGE

The electronic mail system is provided as an organisational communication tool and is owned by the organisation. The organisation reserves the right to monitor all e-mail usage, including opening and reading messages, as required by management and the law. All e-mail usage should therefore be conducted in a responsible, effective and lawful manner. It is important to convey a professional image when using e-mail as a communication tool and special note should be taken to use proper e-mail content, etiquette and speedy replies. To maintain e-mail as an effective and efficient tool, the following must be adhered to:

1. E-mail should primarily be used for business-related purposes. It should not be used for private business activities, personal gain, political activities, fund raising or charitable activities not sponsored by the organisation, amusement or entertainment purposes. Occasional personal use of e-mail is permitted at the discretion of your manager and/or the Chief Information Officer (CIO), which is a privilege that should not be abused;
2. Do not use additional webmail such as hotmail accounts, unless authorised, or access any other private mail accounts from the organisation's System via the Internet, as this could possibly create virus and bandwidth problems;
3. Do not use the e-mail account assigned to another Individual to either send or receive messages. Also do not forge or attempt to forge e-mail messages or disguise or attempt to disguise your identity when sending e-mails;
4. Do not automatically forward your internal organisational mail to external e-mail addresses. You will be held responsible for information security

breaches resulting from this practice;

5. Do not send e-mails to all Users on the global address list;
6. Refrain from sending attachments such as JPEG, JPG and AVI, which have a big impact on bandwidth and are not essential to the business;
7. Do not forward, send or create unsolicited e-mail messages, chain mail or SPAM;
8. Refrain from using the "**Reply to All**" option when responding to e-mail messages, especially when there are more than 10 recipients.
9. Do not knowingly send information in violation of copyright laws.

STORAGE USAGE

The organisation provides disk space on workstations and servers where Users may store organisational information. To ensure that the storage resources are used optimally, the following applies:

1. Only business-related information may be stored on servers and hard drives. Any files not required for business purposes may be deleted on a regular basis at IS's discretion;
2. No workstation drives may be shared, rather use alternative file sharing methods and tools as provided by the organisation;
3. Adhere to the disk quotas assigned to you;
4. Make use of the storage space provided on the network to back-up important files. Files cannot be recovered from a workstation's hard drive should it become faulty.

Removable storage devices can create numerous problems, such as virus infections and copyright infringement, and should therefore be used with care. The following applies:

1. CD/DVD writers are supplied for business and back-up purposes only and may not be used to copy other CDs, DVDs, music, software or other copyright-protected files;
2. Removable storage devices may not be used to copy or distribute CDs, DVDs, music software or other copyright-protected files;
3. Removable storage devices must be scanned for viruses before accessing any files on them;
4. The contents on removable storage devices must be encrypted, where feasible;
5. Removable storage devices must have a form of physical identification on them to ensure that they can easily be recovered and identified.

INAPPROPRIATE CONTENT

The organisation has an important reputation to maintain and as such you must never use your workstation to access, view, distribute, copy or print any material that would be considered “inappropriate” in the work environment. The following includes (without limitation) **inappropriate content** and applies to all IT services, including e-mail and Internet usage:

1. Images of obscene or pornographic content including cartoon graphics, images of mutilation, disfigurement or death, images of a nature which may offend, images of vulgarity, violent or hateful action or images of a racial nature which could cause offence;
2. Messages or text of a sexually-explicit nature including cartoons or jokes, ethnic or racial slurs, defamatory, offensive or abusive statements, or any other messages that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin or religious or political beliefs.

APPENDIX B – SECURITY TESTS

Part 1. Movie Questions

1.1 Does the movie make it clear what is expected of you in terms of Information Security?

□ Not at all

□ To some extent

□ Mostly

□ Completely

1.2 Have you learned something new regarding Information Security from this?

□ Not at all

□ To some extent

□ Mostly

□ Completely

1.3 To what extent do you agree or disagree with this statement: I feel a sense of pride working for TOPAZ CC.

□ Strongly disagree

□ Disagree

□ Neither agree or disagree

□ Agree

□ Strongly Agree

1.4 Which of the following with regard to password practices is considered false?

- ☐ You should never share your password
- ☐ You are allowed to share your password only with an IS technician
- ☐ Your password should not be easily guessable and must contain a mix of alphabet letters and numbers
- ☐ Your password is your key to TOPAZ CC information

1.5 Which of the following statements are correct?

- ☐ When stepping away from your computer, it is permissible to leave it unlocked as long as you switch off the monitor
- ☐ It is acceptable to leave sensitive documents/media on your desk before leaving the office if you put them under a pile of non-sensitive documents
- ☐ When sharing your access details with others, you will not be held responsible for whatever they do with them
- ☐ We must protect customer information at all times

1.6 Which statement most accurately describes TOPAZ CC's Acceptable Usage Policy requirements for passwords:

- ☐ They should be easily guessable so you can remember them
- ☐ They should consist of sequences or repetitive patterns like 1234
- ☐ They should be at least 7 characters in length and contain numbers and letters
- ☐ They should be difficult to guess

1.7 IS personnel call you to inform you that your workstation contains a virus and request your password to address the problem remotely. What do you do?

- ☐ Ignore the request and hang up
- ☐ Provide your password to the person on the line as requested
- ☐ Ask the person for their employee number and then provide the password

□ Do not provide your password and report the incident

1.8 A colleague has requested itemized billing of an TOPAZ CC customer from you. What do you do?

□ Provide the requested information to your colleague

□ Refer the person to your supervisor or manager to ensure that the necessary processes are followed in this regard

□ Ignore the person

□ Extract the information and then ask your supervisor for permission

1.9 Which of the following passwords conforms to the TOPAZ CC Acceptable Usage policy?

□ ab?cd

□ wicked

□ xFj.rQ43

□ michael7

1.10 How can I protect the information in my office:

□ Back up my information daily

□ At the end of the day, lock away my sensitive documents

□ Never leave my workstation unlocked

□ All of the above

Part 2. Movie Questions

2.1 Does the movie make it clear what is expected of you in terms of Information Security?

□ Not at all

□ To some extent

□ Mostly

□ Completely

2.2 Have you learned something new regarding Information Security from this?

□ Not at all

□ To some extent

□ Mostly

□ Completely

2.3 To what extent do you agree or disagree with this statement: TOPAZ CC is better than any other company.

□ Strongly disagree

□ Disagree

□ Neither agree or disagree

□ Agree

□ Strongly Agree

2.4 You learn about a program that you can download from the Internet that enables you to find any song or movie that you want. What do you do?

□ Don't download the program

□ Download the program and scan it for viruses before installing it

□ Search the Internet for reports describing this program

□ Download the program and share it with your friends

2.5 You receive an email message from someone you don't know with the following Subject: "Here is the attachment". The email contains a file attachment called "draft1.doc". What do you do?

□ Open the attachment

□ Save the attachment to disk and scan it for viruses

□ Delete the email without opening the attachment

□ Forward the email to a friend for comments

2.6 According to TOPAZ CC's Acceptable Usage Policy, the composition of your password should:

□ Be at least 5 characters long

□ Not be complex

□ Contain your user ID

□ Not be simple

2.7 Which practices are prohibited at TOPAZ CC?

□ Installing unauthorized or unlicensed software on TOPAZ CC workstations

□ Making copies of TOPAZ CC licensed software and distributing it

□ Interfering with security software on workstations

□ All of the above

2.8 Which of the following are allowed?

□ Disclosing confidential TOPAZ CC information to unauthorised persons

□ Disclosing confidential TOPAZ CC information in public places, for example, by talking on your cell phone in a restaurant

□ Making sure only authorized people have access to confidential TOPAZ CC information

□ If I require information urgently, I can use a computer account for which I do not have authorised access

Part 3. Movie Questions

3.1 Does the movie make it clear what is expected of you in terms of Information Security?

□ Not at all

□ To some extent

□ Mostly

□ Completely

3.2 I know what information security is?

□ Not at all

□ To some extent

□ Mostly

□ Completely

3.3 To what extent do you agree or disagree with this statement: I feel committed to TOPAZ CC.

□ Strongly disagree

□ Disagree

□ Neither agree or disagree

□ Agree

□ Strongly Agree

3.4 You have had a busy weekend so you decide to do your banking and some shopping online during working hours. Which of the following statements are in line with TOPAZ CC's Acceptable Usage policy?

□ You should not do this as it is against company policy

□ You are permitted to do this as long as you get approval from your department head

□ You are permitted to do this as long as the time spent on the Internet does not exceed 30 minutes

□ Formal approval is not required and you are permitted to do this as long as good judgment is followed at all times

3.5 When browsing the Internet a suspicious pop-up window appears. What do you do?

□ Respond to the message in the pop-up window

□ Ensure that your Antivirus software is enabled before clicking on the window

□ Close the pop-up window and ignore the message

□ Click on the window and follow the related prompts

3.6 Which of the following statements are false with respect to Internet usage?

□ Internet usage is provided to you primarily for business use, although occasional use is permitted

□ When using the Internet care must be taken not to access inappropriate material that other employees may find offensive

□ The amount of time you spend on the Internet should be prudent and should not be abused

- □ Once Internet access is granted to you, you are free to access any sites and spend as much time as you like on the Internet

3.7 You receive an email from a friend warning you of a cell phone virus and he asks you to forward this to your friends. What do you do?

- □ Query the message with IS Security if concerned and discard
- □ Reply to the sender of the email thanking them for the information
- □ Send the email to all your TOPAZ CC colleagues
- □ Forward the email to all your friends warning them of the risk

3.8 Which of the following statements are correct?

- □ As the resource owner TOPAZ CC has the right to intercept and view all electronic communication if it obtains a police clearance first
- □ As the resource owner TOPAZ CC has the right to intercept and view all electronic communication if it suspects its systems are being abused
- □ TOPAZ CC is only allowed to monitor Internet activity but not email activity if it suspects abuse by employees
- □ TOPAZ CC is only allowed to monitor email communication and not Internet activity if it suspects abuse by employees

I know of an information security breach within my business area within the last 12 months?

- □ True
- □ False