IGNORANCE TO AWARENESS: TOWARDS AN INFORMATION SECURITY AWARENESS PROCESS

T. Gundu* and S.V. Flowerday**

** Department Information Systems, University of Fort Hare, 50 Church Street, East London, South Africa, 5201 E-mail: tapgun@gmail.com*
*** Department Information Systems, University of Fort Hare, 50 Church Street, East London, South Africa, 5201 E-mail: sflowerday@ufh.ac.za*

Abstract: With most employees in small and medium enterprise (SME) engineering firms now having access to their own personal workstations, the need for information security management to safeguard against loss/alteration or theft of the firms' important information has increased. These SMEs tend to be more concerned with vulnerabilities from external threats, although industry research suggests that a substantial proportion of security incidents originate from insiders within the firm. Hence, physical preventative measures such as antivirus software and firewalls are proving to solve only part of the problem as the employees using them lack adequate information security knowledge. This tends to expose a firm to risks and costly mistakes made by naïve/uninformed employees. This paper presents an information security awareness process that seeks to cultivate positive security behaviours using a behavioural intention model based on the Theory of Reasoned Action, the Protection Motivation Theory and the Behaviourism Theory. The process and model have been refined, tested through action research at an SME engineering firm in South Africa, and the findings are presented and discussed in this paper.

Keywords: Information Security Awareness, Security Behaviour, Information Security Training.

1. INTRODUCTION

SMEs, especially those in the engineering sector, are continually investing significantly in their overall Information and Communication Technologies (ICTs) making Information Security a major concern for the safeguarding of their information assets [10]; [15].

Most of these SMEs have information security policies that present rules to be adhered to [19]. These rules provide a solid foundation for the development and implementation of secure practices within the firms. However, the existence of these formal security policies does not necessarily mean that employees will adhere to the rules [10]. Subsequently, employees need to be aware of the security practices prescribed in the firm's policy.

Information security awareness and training are frequently used for raising awareness of employees and promoting appropriate information security behaviour. This ensures their employees realise the importance of security and the adverse consequences of information security failure plus that there is the potential for people to deliberately or accidentally steal, damage, or misuse data stored within a firm's information systems and throughout the organisation [20]; [45].

Engineering firms rely heavily on digital information stored on networked servers. This information includes patented and unpatented private and confidential designs, plus drawings and client information that are prone to security threats. Engineering SMEs tend to ignore the risk of the uninformed employee and are more concerned with vulnerabilities from external threats; however, industry research suggests that the uninformed employee, by not behaving securely, may expose the firm to serious security risks, for example: data corruption, deletion, and even commercial espionage [1]; [5]; [6]; [22]; [33].

Insider risk can result from two sources: intentional and unintentional behaviour [45]. This paper focuses on unintentional naïve mistakes although intentional dangerous tinkering by disgruntled employees is also a significant threat. Unintentionally uninformed employees (insiders) may expose a firm's information assets to risk by making naïve mistakes, visiting malware infested websites, responding to phishing emails, using weak passwords, storing their login information in unsecured locations, or giving out sensitive information over the phone when exposed to social engineering techniques. Unintentional mistakes by the employee is not an attempt to discredit the firm or make a profit by selling confidential data, but rather as a result of inadequate employee training about information security, that is their lack of security awareness and the consequences of their actions. This weakness can never be totally eliminated, but a well-structured security awareness campaign helps to reduce the risk to acceptable levels [19]; [22].

SME Engineering firms have high levels of trust in their employees not to compromise security; hence, they believe information security awareness is not an issue for them [42]. Ironically, it is more important for SMEs compared to larger firms as employees often have multiple roles and thus have access to a variety of financial, organizational, customer and employee information. Furthermore, there is less segregation of duties in SME engineering firms, thus less control over access to information. Whilst exposed to many of the same threats and vulnerabilities as large organisations,

Based on "The Enemy Within: A behavioural intention model and an information security awareness process", by Tapiwa Gundu and Stephen V Flowerday which appeared in the Proceedings of Information Security South African (ISSA) 2012, Johannesburg, 15 to 17 August 2012.

SMEs do not have access to the same level of resources [42]; this makes their risk even higher.

The purpose of this paper is to present, refine and validate a process that can be followed by SMEs to ensure that their employees are information security aware. This process is mainly based on a behavioural intention model to be presented in section 3.2 and Kruger and Kearney's [21] information security measuring concepts.

The behavioural intention model bases its argument on three principal theories: the Theory of Reasoned Action (TRA) [3], the Protection Motivation Theory (PMT) [28] and the Behaviourism Theory (BT) [47]. Previous works have used research frameworks that integrated TRA, PMT and BT with other theories (even if unconsciously) [10]; [13]; [30]. According to Anderson and Agarwal's [27] review of literature in this area, no prior information security research has used all three theories in a single information security study. Although research has been carried out in the area of information security awareness, there is a lack of literature on the effectiveness of information security awareness methods on the basis of psychological theories as well as a lack of description of the underlying theory of these methods. Psychology is the science of the mind and behaviour. Social psychology has been used for many years for research in the area of education, learning and human behaviour [29].

Action Research was conducted at a civil engineering firm to refine and validate the process. Elden and Chisholm [44] note that action research is change oriented, seeking to introduce changes with positive social values, the key focus of the practice being on a problem and its solution.

The remainder of the paper is organised as follows: first, the information security awareness process is presented, then follows the behavioural intentional model; thirdly, the method for measuring information security is discussed; followed by the analysis and results; finally, the paper concludes by discussing its findings.

2. THE INFORMATION SECURITY AWARENESS PROCESS

Information security theories posit that in order for security efforts to be effective, firms must ensure that employees are part of the security effort [4]; [32]; [34]; [38]; [45].

This section discusses the proposed information security awareness process in the form of a flowchart. Figure 1 shows the proposed information security awareness process for SME engineering firms. The flowchart has four processes (P1, P2, P3 and P4) and three checks (C1, C2 and C3). When planning an information security awareness program, the first step should be to check the existence of an up-to-date Information Security Policy (C1 and C2); however, the firm where the action research was conducted had a sound and up-to-date policy that accurately reflected its overall posture towards information security. The step of drafting or updating an Information Security Policy (P1 and P2) was not carried out and is beyond the scope of this study.

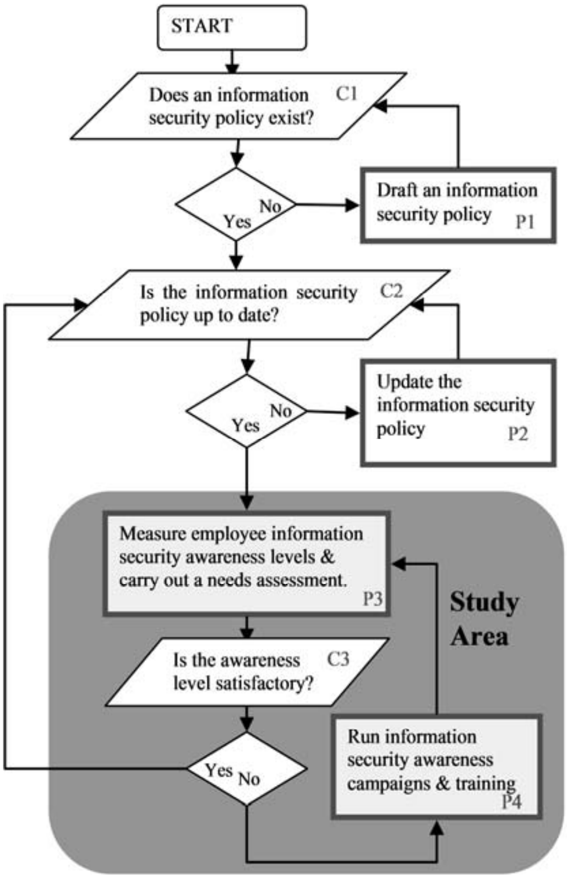

START
Does an information security policy exist?
C1
Yes
No
Draft an information security policy
P1
Is the information security policy up to date?
C2
Yes
No
Update the information security policy
P2
Measure employee information security awareness levels & carry out a needs assessment.
P3
Study Area
Is the awareness level satisfactory?
C3
Yes
No
Run information security awareness campaigns & training
P4

Figure 1: Information security awareness process

The next step is to measure employees' current level of information security understanding (P3) so as to identify any knowledge gaps. During the action research, this needs assessment process highlighted the firm's awareness and training requirements. For example, in the first iteration of the action research, the measurement revealed that employees had an inadequate understanding of password creation, safe Internet usage, virus and firewall understanding, thus highlighting some topics for awareness training. These results also justified to the firm's management the need to allocate resources towards information security awareness and training. The method for measuring employee awareness levels was adapted from Kruger and Kearney's [21] previous research; the details of this method will follow in section 4.

The next step would then be to verify if the current level of information security awareness is at an acceptable level (C3). When conducting the action research, it was found that the level of information security awareness during the first iteration was unsatisfactory and exposed the need for information security awareness campaigns and training. If the levels are unsatisfactory, awareness campaigns and training sessions should be conducted. During the action research, an e-learning based awareness campaign/training was conducted (P4). Its implementation and maintenance is discussed in detail in section 4. The awareness level was measured again after the awareness campaign and results showed that the knowledge gap was closing, but the results were not yet satisfactory according to the scales used (these will be discussed in the data analysis section). The process was then run again for a second and third iteration. The results of the third iteration were satisfactory and the process was stopped.

3. INFORMATION SECURITY AWARENESS CAMPAIGN AND TRAINING (P4)

Awareness from a different perspective: “It is believed that about 200 years ago people did not know about the germ theory; they did not know that they should wash their hands and boil surgical tools to limit the spread of disease and infection. Even though people know these things today, do they always wash their hands before eating, or even after doing something icky?” [39].

Unfortunately, not everyone does so even when they know better. This highlights that the real challenge is not just to teach people, but also to help them change their behaviour. Security knowledge cannot help much if employees do not act on it; hence, this section provides guidelines for implementing and maintaining comprehensive e-learning information security awareness and training campaigns.

Security awareness and training assists in tempering the attitude that security policy is restrictive and interferes with an employee’s ability to do his/her work. The better the employee’s understanding of information security issues, the more they understand the importance of security and the ways in which security protects them and enables them to do their work in a safer and more effective environment [19].

Information security campaigns are divided into awareness and training. Awareness aims to raise the collective knowledge of information security and its controls, while training aims at facilitating a more in-depth level of employee information security understanding. An effective information security awareness and training programme seeks to explain proper rules of behaviour when using the firm’s computer/information systems. The programme communicates information security policies and procedures that need to be followed. Additionally, the campaign imposes sanctions when noncompliance occurs [10].

The BERR 2008 survey [2] suggests that the majority of firms rely upon written materials for training in one form or another. However, simply developing and circulating a policy will not be sufficient to foster appropriate understanding and behaviour. Most companies use the traditional classroom style for awareness and training. However, this study seeks to apply the now widely used tried and tested e-learning concept to information security awareness and training. Jenkins et al [16] and Ricer et al [26] report that there is no significant difference between people who learn using a computer or the traditional classroom style in the short or long-term retention of knowledge.

Additionally this section introduces the behavioural intention model. This model attempts to explain how employee information security awareness knowledge can affect behavioural intentions (towards policy compliance and positive security culture). Behaviourists believe that employees are born with limited innate reflexes (stimulus-response units that do not need to be learnt) and that all of an employee’s complex behaviours are as a result of learning through interaction with the environment [47]. Thus, belief in information security awareness and training should help mould information security behaviours. The information security awareness campaigns and training in P4 on the Information Awareness Process (Figure 1) are based on a behavioural intention model to be explained next.

3.1 Theoretical background of the behavioural intention model

Based on the problems presented in the preceding sections, this section serves to propose, explain and relate the Theory of Reasoned Action (TRA), the Protection Motivation Theory (PMT) and the Behaviourism Theory (BT) to the behavioural intention model.

3.1.1 Theory of Reasoned Action

TRA framework specifically evaluates the relative importance of two incentive components: (1) attitude (2) subjective norm. It suggests that a person's Behavioural Intention (BI) depends on the person's Attitude (A) about the behaviour and Subjective Norms (SN) i.e. (BI = A + SN). Attitude towards behaviour is defined as the individual's positive or negative feelings about performing certain actions. Subjective norm is defined as an individual's perception of whether people important to the individual think the behaviour should be performed. As a general rule, the more favourable the attitude and the subjective norm, the greater the perceived control and therefore the stronger the employee’s intention to perform the behaviour in question [7]; [17]; [23]; [29].

The Theory of Reasoned Action helps to explain how the employee’s attitude towards security and perceived corporate expectation affects the employee’s behaviour towards information security. Consequently, the employee’s attitude and perceived expectations influence the employee’s behavioural intention.

The employee's attitude is affected by cultural, dispositional and knowledge influences. Cultural influences are associated with the employee's background. Dispositional influences are associated with the employee's usual way of doing things. Knowledge influences are associated with the level of knowledge of the subject in question. The employee's attitude can therefore be moulded by information security awareness campaigns and training. The subjective norm is what the employee perceives the firm requires of him/her and perception of how peers would behave in similar scenarios [9]; [13]; [30]. Corporate expectations can therefore be communicated to employees via information security and training sessions. In summary, information security awareness campaigns will help change employee attitudes towards information security and will aid in communicating the firm's expectations to its employees.

3.1.2 Protection Motivation Theory

Protection Motivation Theory (PMT) was developed by Rogers (1983). It was developed from the expectancy value theories and the cognitive processing theories, its aim being to assist and clarify fear appeals. PMT has been noted as one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions [27]. Information security awareness and training instil knowledge in the employees and assists in motivating protection. In essence, protection motivation emanates from both the threat appraisal and the coping appraisal. Threat appraisal describes an individual's assessment of the level of danger posed by a threatening event [28]; [40]. It is composed of perceived vulnerability and perceived severity.

Threat appraisal:

1. Perceived vulnerability i.e. an employee's assessment of the probability of threatening events. In this study it refers to threats resulting from noncompliance with the firm's information security policy (ISP).
2. Perceived severity i.e. the severity of the consequences of the event. In this instance, imminent threats to the firm's information security may arise from noncompliance with the firm's ISP.

The coping appraisal aspect of PMT refers to the employee's assessment of his or her ability to cope with and avoid the potential loss or damage arising from the threat [40]. Coping appraisals are made up of self-efficacy, response efficacy and response cost.

Coping appraisal:

1. Self-efficacy: this factor emphasizes the employee's ability or judgment regarding his or her capabilities to cope with or perform the recommended behaviour. In the context of this paper, it refers to the sorts of skills and measures needed to protect the firm's information assets [11]; [30]; [40].
2. Response efficacy: this factor relates to the belief about the perceived benefits of the action taken by the individual [28]. Here, it refers to compliance with the information security policy as being an effective mechanism for detecting a threat to the firm's information assets.
3. Response cost: this factor emphasizes the perceived opportunity costs in terms of monetary, time and effort expended in adopting the recommended behaviour, in this instance the cost of complying with the ISP. Previous research has used PMT and found it useful in predicting behaviours related to an individual's computer security behaviour both at home and in the work situation [9]; [27], as well as Information Security Policy (ISP) compliance [10]; [30].

3.1.3 The Behaviourism Theory (BT)

Watson coined the term "*behaviourism [47]*." Critical of Wundt's emphasis on internal states, Watson urged psychology to focus on obvious measureable behaviours [47]. Watson believed that theorising thoughts, intentions or other subjective experiences was unscientific [47]. Behaviourism as a theory was primarily developed by Skinner [47]. According to Skinner [47] it loosely encompasses the work of other behavioual researchers like Thorndike, Tolman, Guthrie and Hull.

These investigators had similar underlying assumptions on the processes of learning. These basic assumptions are summarised as follows: First, learning is manifested by a change in behaviour. Second, the environment shapes behaviour. And third, the principles of contiguity (how close in time two events must be for a bond to be formed) and reinforcement (any means of increasing the likelihood that an event will be repeated) are central to explaining the learning process. For Behaviourism, learning is the acquisition of new behaviour through conditioning.

There are two types of possible conditioning:

1. Classical conditioning: where the behaviour becomes a reflex response to stimulus as in the case of Pavlov's Dogs. Pavlov was interested in studying reflexes when he saw that the dogs drooled without the proper stimulus. Although no food was in sight, the dogs still salivated. It turned out that the dogs were reacting to lab coats. Every time the dogs were served food, the person who served the food was wearing a lab coat [49]. Therefore, the dogs reacted as if food was on its way whenever they saw a lab coat. In a series of experiments, Pavlov then tried to figure out how these phenomena were linked. For example, he struck a bell when the dogs were fed. If the bell was sounded in close association with their meal, the dogs learned to

associate the sound of the bell with food. After a while, at the mere sound of the bell, they responded by salivating. Pavlov's work laid the foundation for many other psychologists including Watson's ideas. Watson and Pavlov shared both a disdain for "mentalistic" concepts (such as consciousness) and a belief that the basic laws of learning were the same for all animals whether dogs or humans [49].

2. Operant conditioning highlights reinforcement of behaviour by a reward or punishment. The theory of operant conditioning was developed by Skinner [47] and is known as Radical Behaviourism. According to Reynold [48] the word 'operant' refers to the way in which behaviour 'operates on the environment'. Briefly, a behaviour may result either in reinforcement, which increases the likelihood of the behaviour recurring, or punishment, which decreases the likelihood of the behaviour recurring. It is important to note that, punishment is not considered to be applicable if it does not result in the reduction of the behaviour, and so the terms punishment and reinforcement are determined as a result of the actions. Within this framework, behaviourists are particularly interested in measurable changes in behaviour [48]. In operant conditioning we learn to associate a response (our behaviour) and its consequence and thus to repeat acts followed by good results and avoid acts followed by bad results [48].

3.1.4 The Behavioural Intention Model

Following the preceding discussion, it can be observed that the TRA, PMT or the BT can effect desirable behavioural intention. However, the behavioural intention model in Figure 2 attempts to encourage better behavioural intentions by combining the three theories into one model. Discussions on the behavioural intention model are explained in this section.

Subjective norms have a positive effect on information security policy (ISP) compliance behavioural intention. TRA indicates that individuals' attitudes impact on behavioural intentions [24]. To that end, a positive attitude toward ISP compliance bodes well for good behavioural intention. Conversely, negative attitudes will diminish an individual's ISP compliance and good behavioural intention. Thus, individuals with positive beliefs and values about their firm's ISP might display favourable tendencies towards complying with such rules, requirements and guidelines [10]; [13].

Attitude toward Information Security Policy (ISP) compliance will have a positive effect on ISP compliance behavioural intention. With respect to ISP, it is to be expected that individuals with high information security capabilities and competence will appreciate the need to follow organisational ISPs, and such individuals may be better placed to realise the threats of noncompliance [43].

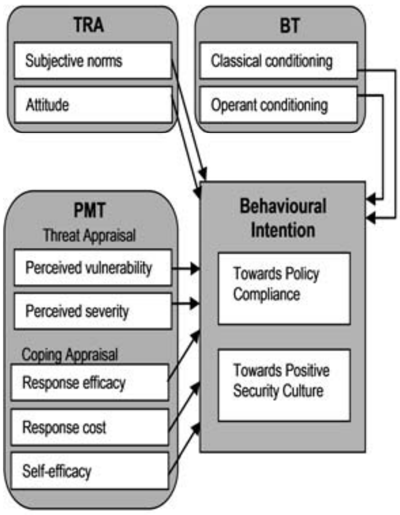


Figure 2: Behavioural intention model

Self-efficacy will have a positive effect on ISP compliance behavioural intention. According to Pahnila et al [30], response costs may include monetary expense, timing inconveniences, embarrassment or other negative consequences, which result from an individual's behaviour. Employees are reluctant to follow or adopt recommended responses if they perceive that a considerable amount of resources i.e. time, effort, and money will be used in pursuit of a low rewarding goal [8]; [9]. Conversely, if small amounts of resources are required in implementing a measure, it may be adopted [36]; [41]. Reducing the Response Cost tends to increase the likelihood of an individual performing a recommended behaviour [40]. Past studies have confirmed that Response Costs are negatively related to intention to use security measures [9]; [41].

Response Cost will have a negative effect on ISP compliance behavioural intention because usually employees believe information security measures are difficult and lengthy.

When an individual possesses requisite knowledge about the effectiveness of a recommended coping mechanism in providing protection from a threat or danger, the individual is more likely to adopt an adaptive behaviour [9]; [28]; [40]. If an individual has doubts regarding the effectiveness of a measure, he or she may not readily accept it [18]. Accordingly, individuals who believe that their organization's ISP has guidelines and coping mechanisms to avert threats and dangers in their context, they are more likely to develop an intention to adopt it [10].

Response efficacy will have a positive effect on ISP compliance behavioural intention. In general, when employees perceive a threat, they often adjust their behaviour in response to the level of risk and determine if they are willing to accept the risk or not [8]; [41]. Thus, an individual's perceived severity tends to be positively linked to their intentions to follow protective actions [36]. If an individual perceives a threat to his or her firm's Information Systems (IS) assets, such an individual will more than likely follow guidelines and requirements laid out in their ISP [13]; [30].

Perceived severity will have a positive effect on ISP compliance behavioural intention with respect to safe computing in the firm; however, individuals who consider themselves immune to security threats are more likely to ignore security measures at work [10]; [13]; [30]. It is reasonable to expect that an individual who perceives high risk to their firm's information system resource will be more likely to adopt protective behaviours.

Therefore, perceived vulnerability will have a positive effect on Information Security Policy (ISP) compliance behavioural intention because employees will be made aware of the vulnerability of the firms' information assets.

3.1.5 Information Dissemination Method (E-Learning)

When information security campaign material based on the needs assessment has been compiled, there is a need to choose a method for communicating the information to the employees. During the action research in this study, an e-learning method was used instead of the conventional classroom style because it provided a configurable infrastructure that integrated learning material, policies, and services into a single solution which quickly, effectively and economically created and delivered awareness and training content. E-Learning allows employees to train at their own convenience and learn at their own pace. It has also proved to be cheaper than bringing everyone together, in terms of time and money. This section therefore seeks to explain how e-learning can be used as a tool for communicating and testing information security awareness training.

E-learning has grown considerably over the past several years as technology has been integrated into education and training. E-learning may be defined as instruction delivered electronically via the Internet, Intranets, or multimedia platforms such as CD-ROM or DVD [35]. The literature review highlighted that research work on e-learning as a tool for information security awareness and training is still in its infancy and that no such tool has been used to date in SMEs.

The e-learning awareness and training program for this study was designed and developed by the researcher with assistance from a multimedia designer and a Web page developer using Macromedia Flash, Macromedia Dream Weaver, PDF, PowerPoint, Access, Gold Wave, and Photoshop software in order to present the program material in a visual and auditory format. This was presented in the form of a website containing information identified by the needs assessment and most relevant recent information security topics. Since information security is a diverse area with many topics, the importance of each topic varies from one firm to another depending on the nature of the risks faced so there is no universal information security awareness training. The training/awareness and testing could be completed in 1-3 hours depending on the speed at which the employee worked. The website for training and awareness was constructed as follows:

> **Home Page:** provides an introduction to information security and the motivation behind the training/ awareness campaign. Employees need to be motivated as to why information security is important. The home page then links to the awareness pages.
>
> **The Awareness/Training Pages:** supply information on topical issues and examples of breaches. These pages contain all the information about information security required by employees.
>
> **The Test Page:** was used as the data collection tool for acquiring data from the employees; this was used to measure their information security awareness levels.
>
> All the pages had attractive information security pictures/video clips/jokes in an effort to create a more relaxed e-learning environment.
>
> The employees participating in the study received an email with instructions on how to use the awareness and training material including a link to the awareness and training website.

E-Learning is a broad term and this paper wishes to stimulate the development of E-Awareness initiatives.

4. MEASURING INFORMATION SECURITY AWARENESS LEVELS (P3)

After the security awareness campaign was launched, it was important to measure its success and draw conclusions from the measured results. Measurement provides evidence of the campaign's effectiveness and reveals where knowledge gaps still exist. Measurements were not limited to a verification of whether the message was received by the target audience, but detected the effectiveness of the message, method and behavioural change.

According to a survey by Richardson [31], 32% do not measure information security awareness in their firms, because there are no commonly agreed and understood standard measurements for the effectiveness of information security awareness campaigns and training. Two distinctive challenges are identified when developing a measuring tool and performing the actual measurements. These challenges are "what to measure" and "how to measure it" [12]; [21].

What to measure:

Kruger and Kearney [21] identified three components to be measured, namely what the employee knows (Knowledge), how they feel about the topic (Attitude), and what they do (Behaviour).

The attitude of employees towards information security is important because unless they believe that information security is important, they are unlikely to work securely, irrespective of how much they know about security requirements. Knowledge is important because even if an employee believes security is important, he or she cannot convert that intention into action without the necessary knowledge and understanding. Finally, no matter what employees believe or know about information security, they will not have a positive impact on security unless they behave in a secure fashion. Figure 3 below shows how enhanced security is achieved by correlating attitude, knowledge and behaviour.

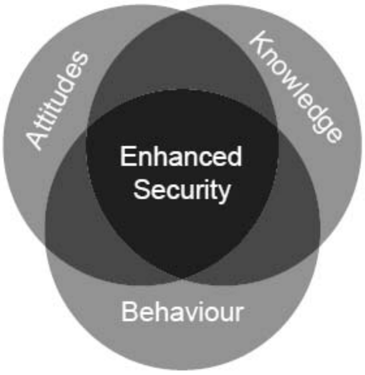


Figure 3: Enhanced Security

How to measure:

Measuring such intangibles as Attitudes, Knowledge and Behaviour is difficult. The action research made use of multiple data collection techniques such as assessment tests, online surveys, participant observation, informal interviews and document surveys for gathering data. However, only the results from online assessment tests were used to calculate security awareness levels; information gathered using the other techniques was only used for needs assessments.

Online Survey and Assessment Tests enable identification of broad trends [14]. An agreement scale was used to allow employees to indicate degrees of agreement with statements about information security.

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

Example statement for test of knowledge:

Internet access to the firm's systems is a corporate resource and should be used for business purposes only.

1.True 2. False 3. Do not know

Example statement to test attitude:

Laptops are usually covered with existing insurance cover so there is no special need to include them in security policies.

1. True 2. False 3. Do not know

Example statement to test behaviour:

I am aware that one should never give one's password to somebody else; however, my work is of such a nature that I do give my password from time to time to a colleague (only to those I trust!).

1. True 2. False 3. Do not know

5. DATA ANALYSIS AND RESULTS

The engineering firm where the action research was conducted was established in 1997. It develops designs, plans, models and geotechnical surveys for the clients it consults. It has thirty two employees, four of whom have no access to the firm's computer resources. This left a sample size of twenty eight employees. The action research was conducted over a ten-month time period from February, 2011 to November, 2011.

In this action research, the researcher was not regarded as an objective, passive outsider. The firm's management expected him to be an active participator, helping to plan and deliver the training program and evaluate its results.
When the information security awareness of the employees was measured for the first time during the needs assessment, only 21% (6 employees) had sufficient levels of information security. Table 1 summarises the information security understanding of the employees per iteration.

Table 1: Employees information security awaremess understanding levels

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

The number of employees with sufficient levels of information security understanding increased on the second iteration due to an increase in knowledge. The majority of employees had sufficient information security understanding after iteration 2 and 3.

All the employees were shown their test results and the overall group results during each iteration in order to motivate those who had not performed well. However, the number of employees showing sufficient levels of

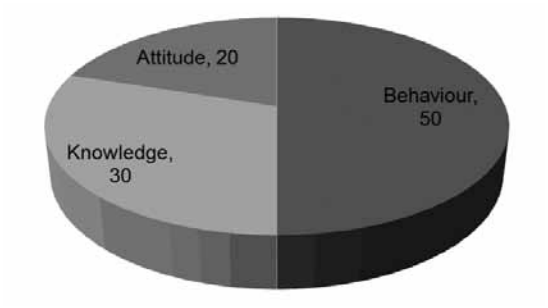


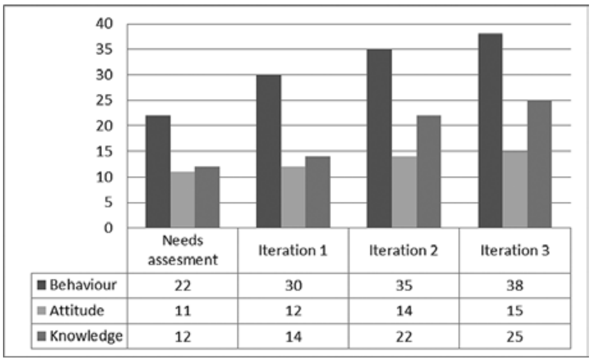
Figure 4: Awareness importance scale [21]

information security understanding is not a true reflection of a firm's overall information security awareness levels; hence Kruger and Kearney's [21] method of analysing data acquired through the measuring methods discussed in the preceding sections was used. This method involved weighting the three aspects being measured in Figure 4.

This weighting was verified with the Managing Director and the Human Resources Manager of the firm who agreed that behaviour was the most important measure followed by knowledge then lastly attitude. The results and importance weightings were processed in a spread sheet application and the output was finally presented in the form of graphs and awareness maps as comparable to Kruger and Kearney's study [21]. Table 2 below shows the scale used to interpret the level of awareness. Kruger and Kearney's scale was slightly modified to take into consideration recommendations by the firm's Managing Director. Figure 5 summarises the results categorised by Knowledge, Attitude and Behaviour.

Table 2: Awareness level measurements [21]

Awareness	Measurement (%)
Good	75
Average	60
Poor	30



	Needs assesment	Iteration 1	Iteration 2	Iteration 3
■ Behaviour	22	30	35	38
■ Attitude	11	12	14	15
■ Knowledge	12	14	22	25

Figure 5: Results summary

The 78% awareness level in the 3rd iteration was satisfactory and there was no need for a fourth although it is advisable to run the process at least once a year as the skills and knowledge of the employees may become outdated.

It was possible to measure the effectiveness of the information security awareness training by using tools and methods outlined by Kruger and Kearney [21]. These enabled the firm to evaluate the extent to which awareness activities had impacted on behaviour, attitude, and knowledge and therefore, whether or not the initial training objectives had been met.

6. FINDINGS

This study confirmed that having and implementing an information security policy does not automatically guarantee that all employees will understand their role in ensuring the security and safeguarding of information assets. It is therefore critical to design and align an information security awareness campaign to the information security policy's high-level goals, objectives and requirements.

The findings of the study support the Theory of Reasoned Action (TRA), the Protection Motivation Theory (PMT) and the Behaviourism Theory (BT). Awareness campaigns were aimed at communicating the firm's stance (subjective norm) on information security, threat appraisal, coping appraisal and in an effort to mould the employees' attitude towards positive behavioural intention. The results showed that an increase in knowledge made a positive change in attitude and behaviour.

However it was discovered that even though initially their security knowledge levels were very low, the employes had a positive attitude towards securing the firm's information assets; however, they did not have the skills and knowledge to behave in a secure manner confirming that the risk to which employees expose a firm is indeed due to unintentional naïve mistakes as was revealed by literature.

What is disappointing is that although knowledge increased dramatically during the iterations, the increase in attitude was marginal. This could be because employees have a certain attitude towards the firm and this attitude cannot be altered by information security awareness alone.

This study revealed that information security awareness programs require the largest portion of the information security budget which should be channelled to the design and implementation of an information security awareness campaign. This supports the findings of Voss [46]. It was revealed that the general costs of running information security awareness campaigns and training can be divided into direct and indirect costs.

Direct costs

- Salary/incentives for the security awareness coordinator or team;
- Training, including instructor fees and room rentals (in the case of classroom style training); and
- Materials, such as slides, web designing, videos, posters, hand-outs and gadgets.

Indirect costs

- Time spent by other employees or departments involved in promoting security awareness; and
- Time spent by the target audience on courses and training.

Making use of e-learning campaign methods significantly reduced the costs of running the awareness campaign. Direct costs involved only the website designing cost, and the firm's in-house technician who was trained on updating and maintaining the website thereafter. Indirect costs reduced as employees took the courses during times they were not busy reducing the chance of productive time being lost.

While carrying out the action research the objectives were to refine and validate the process and change the behaviour of the employees at the particular SME. However, good information security behaviour cultivates an unpredicted information security culture. Hence it can be concluded that good information security awareness campaigns will ultimately result in a positive information security culture.

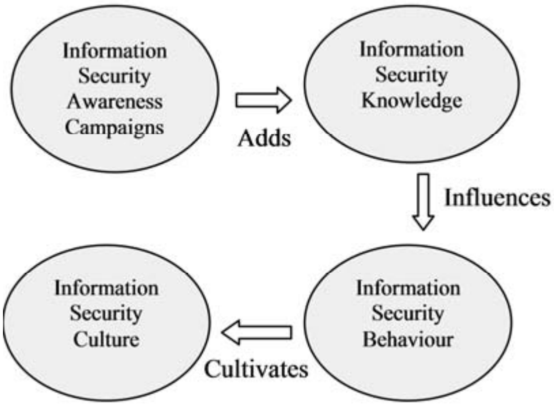

Information Security Awareness Campaigns
Adds
Information Security Knowledge
Influences
Information Security Behaviour
Cultivates
Information Security Culture

Figure 4: From information security awareness to information security culture

7. CONCLUSION

This paper was conceived against the backdrop of efforts made by SME firms to protect their information assets. This paper introduced an information security awareness process, which included behavioural intention models based on three persuasive theories i.e. Theory of Reasoned Action, Protection Motivation Theory and the Behaviourism Theory. The research findings showed that information security awareness levels greatly influence behavioural intentions.

The information security awareness process and behavioural intention was verified through expert review by initially nine information security experts. Additionally, it was refined and validated through action research. After the action research, three more experts reviewed the process and model against the results from the empirical work to further validate them. The information security process yielded positive information security behaviour from employees at the action research host firm during all iterations. The researcher is therefore almost certain that similar results would be achieved if the process and model were put into effect at SMEs with similar characteristics to the one where the study was conducted.

The authors recognise that although e-learning is not a novel idea, it is a relatively new aspect in the field of information security and has great potential to increase e-security awareness initiatives. This study area will become more apparent as e-learning within information security expands. Relating to that, this study has been able to promote e-learning as an effective type of learning compared to the traditional classroom style of learning.

This research study explored the risks exposed by the uninformed naïve employee to SME firms' information assets. However, the risks exposed by the malicious insider as well as the outsider still require further exploration.

8. REFERENCES

[1] R.Willson and M. Siponen. "Overcoming the insider: reducing employee computer crime through situational crime prevention", *Communications of the ACM*. Vol 52(9), September 2009. NY, USA.

[2] BERR. "Information Security Breaches Survey" – *Technical Report*. Department for Business Enterprise & Regulatory Reform. April 2008. URN 08/788.

[3] M. Fishbein, and I. Ajzen. *Belief, attitude, intention, and behaviour: An introduction to theory and research*, Massachusetts: Addison-Wesley, 1975.

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

[5] S. Furnell. "Malicious or misinformed? Exploring a contributor to the insider threat," *Computer Fraud & Security*. Vol 2006(9), pp 8-12, September 2006.

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

[7] J.L. Hale, B.J. Householder and K.L. Greene. The theory of reasoned action. In J. P. Dillard, and M. Pfau, *The persuasion handbook: Developments in theory and practice* (pp. 259 – 286). Califonia: Thousand Oaks, 2003.

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

[9] Y. Lee and K.R. Larsen. “Threat or coping appraisal: determinants of SMB executives’ decision to adopt anti-malware software,” *European Journal of Information Systems*, Vol 18(2), pp 177-87, 2009.

[10] T. Herath and H.R. Rao. “Encouraging information security behaviours in organizations: Role of penalties, pressures and perceived effectiveness,” *Decision Support System*, Vol 47, pp 154 – 165, 2009.

[11] A. Bandura. “Social cognitive theory of self-regulation,” *Organizational Behaviour and Human Decision Processes*, Vol 50, pp 248-87, 1991.

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

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

[14] E. Hofstee. Literature Review. *In constructing a good dissertation.* Johannesburg: EPE, 2006.

[15] ISACA. (2009). An Introduction to the Business Model for Information Security. California. Available from: http://www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm &ContentID=48017 (Accessed 3 February 2010).

[16] S. Jenkins, R. Goal and D. Morrele. “Computer-assisted instruction versus traditional lecture for medical student teaching of dermatology morphology: A randomized control trial,” *Journal of the American Academy of Dermatology*. Vol 59(2), pp 255−259, 2008.

[17] K. Miller. Communications theories: perspectives, processes, and contexts, New York: McGraw-Hill, 2005.

[18] P.A. Rippetoe and R.W. Rogers. “Effects of components of protection motivation theory on adaptive and maladaptive coping with a health threat,” *Journal of Personnel Social Psychology*. Vol 52, pp 596-604, 1987.

[19] E. Johnson. “Security Awareness: Switch to a better program,” *Network Security*. Vol 6, pp 15-18, 2006.

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

[21] H.A. Kruger and W.D. Kearney. “A Prototype for assessing information security awareness,” *Computers & Security*. Vol 25(4), pp 289 – 296, 2006.

[22] R.L. Krutz and D.V. Rusell. *The CISP Prep Guide*. New York: John Willey & Sons, 2001.

[23] K. Miller. *Communications theories: perspectives, processes, and contexts*. New York: McGraw-Hill, 2005.

[24] I. Ajzen. “The theory of planned behaviour”. *Organizational Behaviour and Human Decision Processes*. Vol 50(2), pp 179-211, 1991.

[25] R. Power. “CSI/FBI Computer Crime and Security,” *Computer Security Journal*, Vol 17, pp 7-30, 2002.

[26] R.E. Ricer, A.T. Filak, and J Short. “Does a high tech (computerized, animated, PowerPoint) presentation increase retention of material compared to a low tech (black on clear overheads) presentation?” *Journal of Teaching and Learning in Medicine*. Vol 17(2), pp107−111, 2005.

[27] C.L. Anderson and R. Agarwal. “Practicing safe computing: a multimethod empirical examination of home computer user security behavioural intentions,” *MIS Quarterly*. Vol 34(3), pp 613-43, 2010.

[28] R. Rogers. Cognitive and physiological processes in fear-based attitude change: a revised theory of protection motivation. In: J. Cacioppo, R. Petty, editors. *Social psychophysiology: a sourcebook*. New York: Guilford Press, pp 153-76, 1983.

[29] M.A. Hogg and D. Abrahams, Social identifications: A social psychology of intergroup relations and group processes. Routledge London and New York, 1988.

[30] S. Pahnila, M. Siponen and A. Mahomood. “Employees’ behaviour towards IS security policy compliance,” *Proceedings of the 40th Hawaii International Conference on System Sciences*, January, pp 3-6, Los Alamitos, CA; 2007.

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

[32] C. Russell. “Security Awareness - Implementing an Effective Strategy,” SANS Institute, *InfoSec Reading Room,* 2002.

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

[34] B. Schneier. Schneier on Security. New Jersey: John Wiley & Sons, 2008.

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

[36] C. Pechmann, G. Zhao, M. Goldberg and E.T. Reibling E.T. “What to convey in antismoking advertisements of adolescents: the use of protection motivation theory to identify effective message themes,” *Journal of Marketing.* Vol 6, pp 1-18, 2003.

[37] J. Van Niekerk and R. von Solms. “Organisational Learning Models for Information Security,” *Peer reviewed Proceedings of the ISSA 2004* enabling tomorrow conference 30 June – 2 July 2004, Gallagher Estate, Midrand.

[38] J. Van Niekerk and R. von Solms. “Information Security Culture: a management perspective.” *Computers & Security*. Vol 29(4), pp 476-86, 2010.

[39] H. William. “Methods and techniques of implementing a security awareness program”. *SANS Institute, InfoSec Reading Room*, 2002.

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

[41] M. Workman, H.H. Bommer and D. Straub. “Security lapses and the omission of information security measures: a threat control model and empirical test,” *Computers in Human Behaviour*. Vol 24, pp 816, 2008.

[42] P.A.H. William. “In a ‘trusting’ environment, everyone is responsible for information security.” *Information Security Technical report*. Vol 13, pp 207 – 215, 2008.

[43] P. Ifinedo. “Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory,” C*omputers & Security.* Vol 31(1), pp 83-85, 2012.

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

[45] J. Cox. “Information systems user security: A structured model of the knowing–doing gap.” *Computers in Human Behaviour.* Vol 28, pp 1849–1858, 2012

[46] B.D. Voss. “The Ultimate Defense of Depth: Security Awareness in Your Company”. *SANS Institute, InfoSec Reading Room*, 2001.

[47] B.F. Skinner. *Science and human behaviour*. New York: Free Press, 1965.

[48] G.S. Reynold. *A primer of operant conditioning*. (Rev Ed) Michigan: Scott, Foresman, 1975.

[49] A.W. Staats, and C.K. Staats. "Attitudes established by classical conditioning." *The Journal of Abnormal and Social Psychology.* Vol 57(1), pp 37-48, 1958.