The Enemy Within:

A Behavioural Intention Model and an Information Security Awareness Process

Tapiwa Gundu
Department Information Systems
University of Fort Hare
East London, South Africa
tapgun@gmail.com

Stephen V Flowerday
Department Information Systems
University of Fort Hare
East London, South Africa
sflowerday@ufh.ac.za

***Abstract*—Most employees in small and medium enterprise (SME) engineering firms now have access to their own personal workstations which have become part of their daily functions. This has led to an increased need for information security management to safeguard against loss/alteration or theft of the firm's important information. SMEs tend to be concerned with vulnerabilities from external threats, although industry research suggests that a substantial proportion of security incidents originate from insiders within the firm. Hence, physical preventative measures such as antivirus software and firewalls are proving to solve only part of the problem as the employees controlling them do not have adequate information security knowledge. This tends to expose the firm to costly mistakes that can be made by naïve/uninformed employees. This paper presents an information security awareness process that seeks to cultivate positive security behaviours using the behavioural intentions models i.e. the Theory of Reasoned Action and the Protection Motivation Theory. The process presented has been tested at an SME engineering firm, and findings are also presented and discussed in this paper.**

Keywords- Information Security Awareness; Security Behaviour

I. 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 providing a solid foundation for the development and implementation of secure practices within the firms. These policies present the rules that must be adhered to [19]. The existence of these formal security policies does not necessarily mean that employees will adhere to the rules [10]. Subsequently, the employees need to be aware of the security practices prescribed in the policy. Information security awareness and training are frequently used for training employees towards safe information security behaviour. This ensures employees realise the importance of security and the adverse consequences of security failure and 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].

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

An uninformed employee (insider) may expose the firm's information assets to risk by making naïve mistakes, visiting malware infested websites, responding to phishing emails, using weak passwords, storing their login information in unsecured locations, or giving out sensitive information over the phone when exposed to social engineering techniques. The unintentional insecurity 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 on security, or lack of security awareness of the consequences of their actions. The weakness they present can never be totally eliminated, but a well-structured security awareness campaign helps to reduce the risk to acceptable levels [19]; [22].

The insider risk to the firm can be divided into 2 categories, intentional and unintentional risk. This paper focuses on unintentional insecurity/naïve mistakes although intentional insecurity/dangerous tinkering by disgruntled employees is also significant. This is an area still open for further research.

SME engineering firms often assume significant trust levels from employees; 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 as well access to multiple services such as the Internet and email. Furthermore, there is less segregation of duties in SME engineering firms, thus less control over access to information. Whilst exposed to the same threats and vulnerabilities as large organisations, SMEs also do not have access to the same level of resources [42]; this makes their risk even higher than larger organisations.

This paper bases its argument on two principal theories, the Theory of Reasoned Action (TRA) [3] and the Protection Motivation Theory (PMT) [28]. Previous works have used

research frameworks that integrated TRA and PMT with other theories (e.g. [13]; [10]; [30]). According to Anderson and Agarwal's [27] review of literature in this area no prior information security research has used both theories in a single information security study.

The purpose of this paper is to examine the factors that influence employee behaviour towards information security and present a practical design of an information e-learning based security awareness process that can be used by SME engineering firms in order to cultivate positive employee information security behaviour. The remainder of the paper is organised as follows: first, information about the study's theoretical foundation is presented; second, presentation of the proposed information security awareness process; next, information about the analysis and results is presented; the paper concludes by discussing its findings.

II. THEORETICAL BACKGROUND

Based on the problem presented in the preceding section, this section serves to propose, explain and relate the Theory of Reasoned Action (TRA) and the Protection Motivation Theory (PMT) to the study.

2.1 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 a behaviour. Subjective norm is defined as an individual's perception of whether people important to the individual think the behaviour should be performed. As a general rule, the more favorable the attitude and the subjective norm, the greater the perceived control and therefore the stronger the employee's intention to perform the behaviour in question [7]; [23]; [17]; [29].

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

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

2.2 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 the following two items:

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

(ii) Perceived severity i.e. the severity of the consequences of the event. In this instance, imminent threats to the firm's information security arising from noncompliance with the firm's ISP.

The coping appraisal aspect of PMT refers to the employee's assessment of his or her ability to cope with and avoid the potential loss or damage arising from the threat [40]. Coping appraisals are made up of three sub constituents:

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

III. THE RESEARCH MODEL

Following the preceding discussion, the research model implemented in this study is presented in Figure. 1. It can be

observed that both the TRA and PMT can be fused to effect desirable behavioural intention. Discussions on the research hypotheses are represented next.

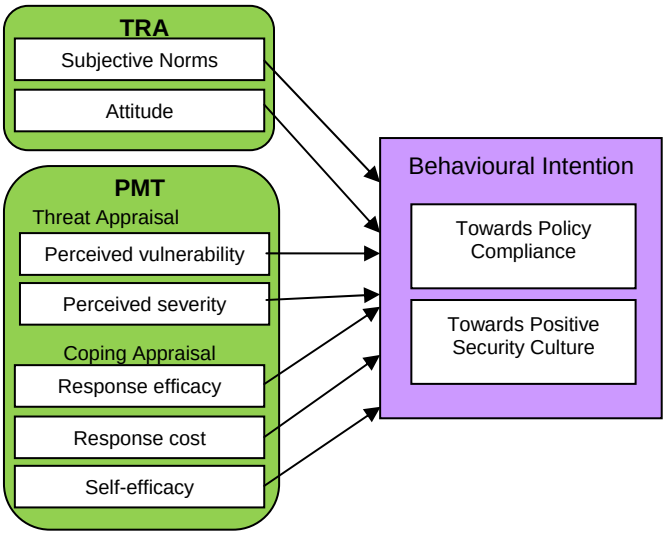

Figure 1: Behavioural Intention Model

Subjective norms will have a positive effect on ISP compliance behavioural intention. TRA indicates that individuals' attitudes impact behavioural intentions [24]. To that end, a positive attitude toward ISP compliance bodes well for ISP compliance and good behavioural intention. Conversely, negative attitudes will diminish an individual's ISP compliance and good behavioural intention. Thus, individuals with positive beliefs and values about their firm's ISP will display favourable tendencies towards complying with such rules, requirements, and guidelines [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 organizational ISPs and such individuals may be better placed to realise the threats of noncompliance [43].

Self-efficacy will have a positive effect on ISP compliance behavioural intention. According to Pahnila et al. [30], response costs may include monetary expense, timing inconveniences, embarrassment or other negative consequences, which result from an individual's behaviour. Employees are reluctant to follow or adopt recommended responses if they perceive that a considerable amount of resources i.e. time, effort, and money will be used toward a 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 [41]; [9].

Response cost will have a negative effect on ISP compliance behavioural intention. When an individual possesses requisite knowledge about the effectiveness of a recommended coping mechanism in providing protection from a threat or danger, the individual is more likely to adopt an adaptive behaviour [28]; [40]; [9]. On the other hand, if the individual has less belief 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 behaviours in response to the amount of risk and determine if they are willing to accept the threat 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 view themselves immune to security threats are more likely to ignore security measures at work [10]; [13]; [30]. On the other hand, it is reasonable to expect that an individual who perceives high vulnerability to their firm's information system resource will be more likely to adopt protective behaviours.

Therefore, perceived vulnerability will have a positive effect on Information Security Policy (ISP) compliance behavioural intention.

IV. Methodology - (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 efforts [4]; [38]; [32]; [34].

Having discussed the theoretical background of the study, this section discusses the proposed information security awareness process in the form of a flow chart. The process is based on the Behavioural Intention Model discussed. This process was verified through expert review and tested through action research. The Action research was conducted at an SME civil engineering firm in South Africa. Three iterations of the processes indicated above were conducted to verify the outcome of the results.

The process starts by checking the existence of an up to date Information Security Policy (ISP); however, the firm at which 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/updating an Information Security Policy (ISP) was not carried out and is beyond the scope of this study. Figure 2 shows the proposed

information security awareness process for SME engineering firms.

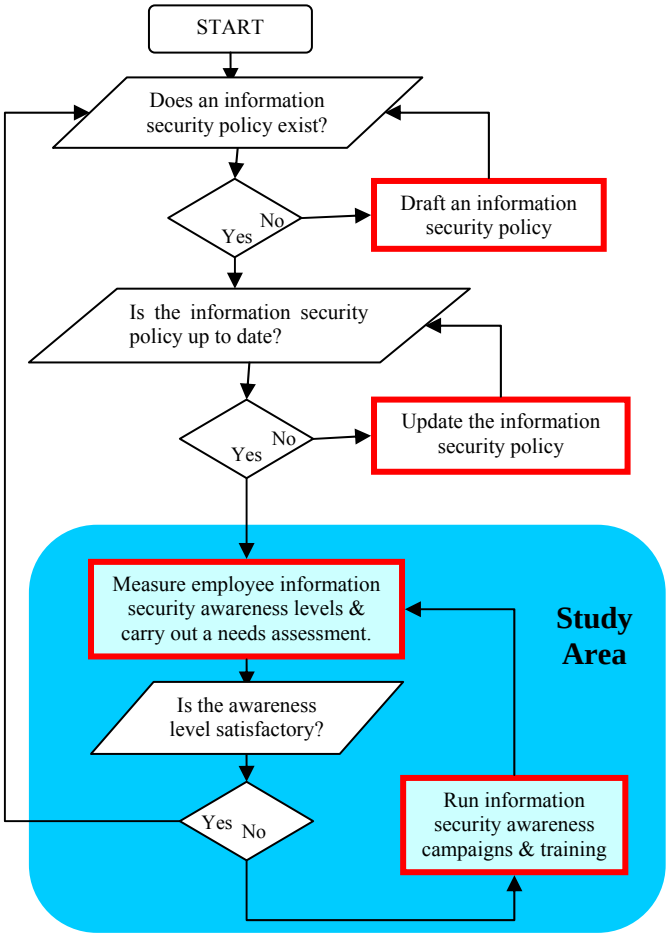

Figure 2: Information security awareness process

The next step was to measure employees' current level of the information security understanding so as to expose any knowledge gaps. This needs assessment process highlighted the firm's awareness and training needs. For example, in the first iteration of the action research, the measurement revealed that employees did not have adequate understanding of password creation, safe Internet usage, viruses and firewalls, 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 4.3.

The awareness levels during the first iteration were unsatisfactory and exposed the need for information security awareness campaigns and training. An e-learning based awareness campaign was carried out. Its implementation and maintenance is discussed in detail in section 4.2. 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 time. The results of the third iteration were satisfactory and the process was stopped.

4.1 Information Security Awareness Campaign and Training

Awareness from a different perspective: "It is believed that about 200 years ago people did not know about the germ theory; they did not know that they should wash their hands and boil surgical tools to limit the spread of disease and infection. Even though people know these things today, do they always wash their hands before eating, or even after doing something icky?" [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 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. This must precede and impose sanctions when noncompliance occurs [10].

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

An e-learning system was used in this study instead of the conventional classroom style because it provides a configurable infrastructure that integrates learning material, policies, and services into a single solution to quickly, effectively, and economically create and deliver awareness and

training content. E-Learning allows employees to train at their own convenience, and learn at their own pace. It has also proved to be cheaper than bringing everyone together, in terms of time and money. The next section therefore seeks to explain how e-learning can be used as a tool for communicating and testing information security awareness training.

4.2 Implementation method (E-Learning)

The information security awareness communication path used was E-Learning. E-learning has grown tremendously over the past several years as technology has been integrated into education and training. E-learning may be defined as instruction delivered electronically via the Internet, intranets, or multimedia platforms such as CD-ROM or DVD [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 by using Macromedia Flash, Macromedia Dream Weaver, PDF, PowerPoint, Access, Gold wave, and Photoshop software in order to present the program material in a visual and auditory format. This was presented in the form of a website containing information identified by the needs assessment and most relevant information security topics. Since information security is a diverse area with many topics, the importance of each topic varies from one firm to another depending on the nature of the risks faced so there is no universal information security awareness training. The website for training and awareness was constructed as follows:

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

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

The Test/Exam Page: this was used as the data collection tool for acquiring data from the employees which was used to measure their information security awareness levels.

All the pages had attractive information security pictures/video clips/jokes in an effort to create a more relaxed e-learning environment.

The employees participating in the study received an email with instructions on how to use the awareness and training program including the link to the awareness and training website.

4.3 Measuring information security awareness levels

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

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

4.3.1 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 behavior.

Figure 3: Enhanced Security

4.3.2 How to measure

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

Online Surveys (assessment tests) Assessment tests enable identification of broad trends [14]. An agreement scale was used to allow the employees to indicate degrees of agreement with statements about security.

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

Example statement for test of *knowledge*:

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

1.True 2. False 3. Do not know

Example statement to test *attitude*:

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

1. True 2. False 3. Do not know

Example statement to test *behaviour*:

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

1. True 2. False 3. Do not know

V. Data Analysis and Results

The engineering firm where the action research was conducted has 32 employees of whom 4 have no access to the firm's computer resources. This left a sample size of 28 employees.

When the information security awareness of the employees was measured for the first time during needs assessment, only 21% (6 employees) passed with a score above 50%. The number of employees passing on the second iteration increased, this was due to the increase in knowledge. The iteration 2 and 3 a huge majority of the employees passed the test. Figure 4 shows how many employees passed per iteration.

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

Figure 4: Employees passing awareness test

However the number of employees passing is not a true reflection of the firms overall information security awareness levels hence Kruger and Kearneys [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 as follows (Figure 5):

Dimensions	Weighting (%)
Knowledge	30
Attitude	20
Behaviour	50

Figure 5: Awareness importance scale [21]

This weighting was verified with the 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 weights were processed in a spreadsheet application and the output was finally presented in the form of graphs and awareness maps as was done in Kruger and Kearney's [21] study. Figure 6 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 firms Director.

Awareness	Measurement (%)
Good	75
Average	60
Poor	30

Figure 6: Awareness level measurement [21]

Due to paper length constraints a detailed discussion of the outcomes of the research cannot be presented here; however, Figure 7 below summarises the results categorised by the knowledge, attitude and behaviour.

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

Figure 7: Results of three iterations of the information security process

The 78% awareness level was satisfactory and there was no need for a forth iteration although it will be advisable to run the program at least once a year as the skills and knowledge the employees might become outdated.

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

VI. FINDINGS

This study revealed that having and implementing an information security policy does not automatically guarantee that all employees 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) and the Protection Motivation Theory (PMT). Awareness campaigns were aimed at communicating the firm's stance (subjective norm) on security, threat appraisal coping appraisal and try to mould the employees' attitude towards positive behavioural intention. The results showed that an increase in knowledge, made a positive change in attitude and behaviour.

However it was discovered that even though initially the employees' security knowledge levels were very low. They had a positive attitude towards securing the firms information asset; however, they did not have the skills and knowledge to help them behave in a secure manner. This also helps to advocate that indeed the risk the employees expose the firm to is genuinely unintentional but naïve mistakes as was revealed by the literature review.

The study has also discovered the need to run the process within 12 months as the information systems area is changing and so do the risk and security measures that need to be taken. It is also important to run the process for all new employees hired as it is best to initiate information security training and awareness during new-hire orientation to establish the firm's commitment to security at an early stage of their employment.

What is disappointing is that although knowledge increased dramatically during the iterations, the increase in attitude was marginal. This is most likely because the employees have a certain attitude towards the firm and this attitude cannot be altered by information security awareness. Most probably looking at job satisfaction might be able to change employee attitude towards the firm.

VII. CONCLUSION

This paper was conceived against the backdrop of efforts made by SME firms to protect their information assets. Firms usually procure technological tools to help them achieve success on business fronts.

As an underlying theoretical background in the area, this paper drew on two relevant theories which included behavioural intention and persuasive theories i.e. Theory of Reasoned Action and Protection Motivation Theory. The research findings showed that information security awareness levels are greatly influenced by behavioural intentions.

The study has also been able to prove e-learning as an effective type of learning just as the traditional classroom style of learning.

In conclusion the model and process presented in this Paper have been successfully validated by the action research conducted. This is proven by the positive change in behaviour observed during the iterations.

Future research could focus on models and theories that assist in improving employee attitude as the behavioural intention model has proven to only be able to impact on knowledge and behaviour and not the employees' attitude.

VIII. REFERENCES

[1] R.Willson & M. Siponen. "Overcoming the insider: reducing employee computer crime through situational crime prevention", *Communications of the ACM*. Vol 52, 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 behavior: An introduction to theory and research*," Massachusetts: Addison-Wesley, 1975.

[4] A. Da Veiga and J.H.P. Eloff. A "Framework and assessment instrument for Information Security Culture," *Computers & Security*, 29(2), 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, Issue 2, pp 5-10, February 2009.

[7] J.L. Hale, B.J. Householder and K.L. Greene, K. L. 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, S. Orbell. "Prediction and intervention in health-related behavior: a meta-analytic of protection motivation theory," *Journal of Applied Social Psychology*, Vol 30(1), pp 106-43, 2000.

[9] Y. Lee, 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 behaviors 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 Behavior 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, Accesed Feb. 2010, Available at: http://www.noticebored.com/html/metrics.html

[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 contol 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, p 596, 1987.

[19] E. Johnson. “Security Awareness: Switch to a better program,” *Network Security*. Vol 2006, 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, 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 behavior”. *Organizational Behavior 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 behavioral intentions,” *MIS Quarterly*. Vol 34, 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] J.L. Hale, B.J. Householder and K.L. Greene. The theory of reasoned action. In J.P. Dillard & M. Pfau (Eds.), The persuasion handbook: Developments in theory and practice (pp. 259–286). Thousand Oaks, CA: Sage, 2003.

[30] S. Pahnila, M. Siponen and A. Mahomood. “Employees’ behavior 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 ET. “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, 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 Behavior*. 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 behavior and the protection motivation theory,” C*omputers & Security.* Vol 31, pp 83-85, 2012.