THE IMPACT OF INFORMATION SECURITY AWARENESS TRAINING ON INFORMATION SECURITY BEHAVIOUR: THE CASE FOR FURTHER RESEARCH

AT Stephanou[1], R Dagada[2]

[1, 2] University of the Witwatersrand
tony.stephanou@gmail.com
rabelani.dagada@wits.ac.za

ABSTRACT

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

Research carried out on information security has traditionally been slanted towards technical aspects of security, typically rooted in computer science and mathematics. Security was traditionally seen as a service to be provided and not something that was influenced by users. However, it was soon recognised that focusing on technical issues alone is inadequate. Technologies meant to provide security ultimately depend on the effective implementation and operation of these technologies by people. Thus awareness of policies is needed by all individuals in an organisation to ensure that policies are well understood and not misinterpreted. Some

researchers have maintained that educating users is futile mainly because it is believed that it is difficult to teach users complex security issues and secondly, because security is seen as secondary by the user they will not pay enough attention to it. This paper reflects research in progress and discusses some of the problems with existing information security awareness research and proposes a model to be tested for examining the impact of information security awareness training on information security behaviour.

KEYWORDS

Information security, behavioral information security, awareness initiatives, on the job behaviours, policies, and further research.

THE IMPACT OF INFORMATION SECURITY AWARENESS TRAINING ON INFORMATION SECURITY BEHAVIOUR: THE CASE FOR FURTHER RESEARCH

1 INTRODUCTION AND BACKGOUND

Information Technology systems are dependant on people. Schneier (2003:10) maintains that information security is more about behaviour than anything else, i.e. getting people to behave in a certain way. It is people's intentional and unintentional actions that cause adverse consequences that security wants to prevent. Despite the hype from vendors about the need for security products many critical security activities have not and cannot be automated. Technologies meant to provide security ultimately depend on the effective implementation and operation of these technologies by people. This means that organisations are dependant on people to achieve a secure environment. Since humans are seen as the "weakest link" in the information security chain (Schneier, 2000; Stanton et. al. 2003:1; Katsikas, 2000:130; van Niekerk & von Solms, 2004:2; von Solms, 2000:618), there is a clear requirement to ensure users are trained correctly in terms of information security policies. The goal is to ensure that users use the necessary policies and to ensure that they are not misused or misinterpreted, thereby ensuring the effectiveness of policies (Siponen, 2000:31). Security awareness efforts are seen as the "first line of defence" (OECD, 2002:10). On the other hand, Van Niekerk & von Solms (2004), argue that awareness initiatives while necessary are not sufficient to obtain the desired results, while other authors simply consider educating users futile (Ranum, 2005; Evers, 2007; Nielsen, 2004).

Well established security management standards such as the SABS ISO/IEC 17799 and the OECD guidelines for information systems security also promote the importance of making people aware of security issues. The 2007 Computer Security Institute (CSI) Survey reported a substantial

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

Despite the understanding that awareness is important, it is not beyond doubt whether a clear message is being communicated to users in the first place (Gaunt, 2000:152-153). This is especially true for dynamic, complex threats such as phishing attacks. Srikwan & Jakobsson (2007), for example, doubt whether a clear message is being communicated to users with respect to identity theft, specifically on what to do and why it must be done – even though a vast amount of guidance on this subject is being directed at users. South African banking clients for example are frequently warned about the threat of phishing scams (via email, SMS and so on). Are these interventions having an effect? Perhaps, there may be too much information for lay people to digest and security practitioners may be unwittingly shooting themselves in the foot.

With all this emphasis on awareness, the question one has to ask is: to what end? In other words, does making users more aware lead to more secure behaviour and therefore contribute to a more "secure" organisation or, are awareness campaigns doomed to fail?

The purpose of this paper is two-fold. Firstly, it will be demonstrated that there is a shortage of in-depth information security awareness research and that behavioural concepts are not properly taken into account for security awareness programmes. Next, this paper represents research in progress aimed at explaining and answering some of the questions raised above. A theoretical model is put forward proposing how a particular security awareness approach affects behaviour. This will help scholars and practitioners understand why an awareness initiative is expected to have certain results on security behaviour. The theory proposed will be then be tested empirically using a pretest-posttest experimental design. The authors believe that the contribution of this research is significant in the following ways: The research is a case study that will use system generated data to measure actual user behaviour before and after the security awareness

training intervention in order to determine effectiveness of the training. Therefore the perceptions of users about their own behaviour will not be relied upon. Existing research has used interviews, surveys and "participatory observation" to make conclusions about end-user behaviours in this regard. The research will measure a subset of behaviours required by a typical Acceptable Usage Policy, whereas much of the existing and recent research with respect to awareness training effectiveness has focused on phishing related threats. The research in progress intends to not only demonstrate the impact of security awareness training on user behaviour but to also contribute towards a set of instruments that could be used in future research for behavioural measurement. Finally, the study underway, uses as a foundation, the user behaviour taxonomy developed by Stanton et. al. (2005) in an effort to begin to consolidate the security awareness research landscape and move towards a common understanding and language of what "security behaviour" means.

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

Figure 1 demonstrates one way of making sense of the available information security research. Most of the research work can be placed into one of these categories. This paper will not discuss research focused on computer abuse or the insider threat.

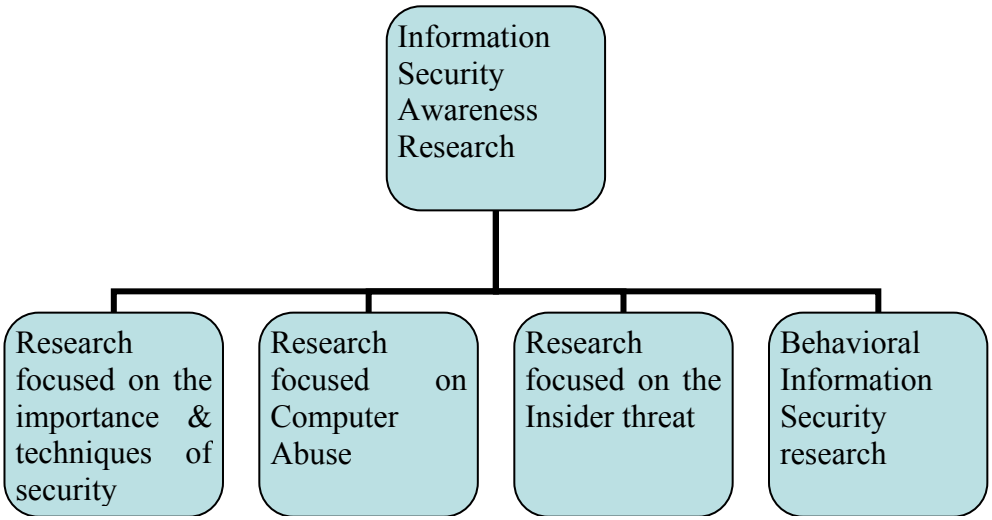

Figure 1: Information Security Awareness Landscape

2 RESEARCH FOCUSED ON THE IMPORTANCE & TECHNIQUES OF SECURITY AWARENESS

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

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

Srikwan & Jakobsson (2007), argue that educational efforts generally expect too much from the audience while others – in an effort to make the message more palatable – simplify the message to such an extent that the meaning is diluted. Without an adequate understanding of security requirements and their support, security processes are bound to be

ineffective (Van Niekerk & von Solms, 2004). For example, a well-crafted incident management process is useless if an employee is not aware of firstly what a security incident looks like and then how to respond to the incident when one is recognised. Ultimately, security education in this context becomes inadequate. Thus security awareness practitioners need to ensure that there is a connection made between what a user knows and what the appropriate behaviour expected from them is. In order for security to be enhanced they need to be told not only what to do but why they should do it.

The problem may be more complex than originally anticipated by security practitioners. Perhaps the solution is not only to deploy awareness campaigns and educate users, but more related to the notion of the ability of users to understand risk and make trade-offs (Schneier, 2003:17) and naturally wanting to be helpful (Mitnick & Simon, 2003). Most of the time people are told what to do without explaining why they need to do this. This is linked to people's understanding of threats. If they are able to understand the underlying threat then they will be able to look for patterns and consequently mitigate any threat posed (Srikwan & Jakobsson 2007).

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

Despite these challenges, Kumaraguru et. al (2007) showed that security awareness material – when used - can be effective. They found that online material that informs users about the threats of phishing was highly effective – resulting in users getting better at identifying phishing sites. They also call for looking at more effective techniques to deliver the awareness message, getting users to actually read and absorb the material and, ensuring more work is done on the quality of awareness materials presented.

Jagatic et. al. (2007:96) also used contextual training. They demonstrated that a large amount of information (accessible via social networking sites on the Internet) was easily obtainable and could effectively

be used for phishing attacks. The researchers also wanted to measure how social context information could influence the success of phishing attacks. The difference with this research is that they tricked their users by spoofing emails that looked like it came from friends in their social network. The number of students that fell prey to the (harmless) phishing attack was 72% (out of 487 targeted students) – this was much higher than anticipated (Jagatic et. al., 2007:97).

To summarise, previous research on information security awareness has been skewed towards awareness techniques, computer abuse and insider threats. Although recent research has started examining the effectiveness of security awareness the focus has been on phishing threats, which has shown the effectiveness of class-room based training, phishing tests, email based training and web-based awareness material. Measuring the effectiveness of overall security awareness and examining behavioural aspects have been largely neglected. In addition, very few theoretical models have been presented and used to explain and test security behaviours.

3 BEHAVIORAL INFORMATION SECURITY

The importance of getting people to act correctly has always been implied by previous research work. However, a few years ago there has been more explicit focus on behavioural aspects of security. Behavioral information security is a branch of information security research which examines what motivates security related behaviours of computer users. Recent work in behavioral information security has shown: how employee job attitude relates to information security behaviours (Stanton et. al., 2003); what categories of information security behaviours exist (Stanton, et. al., 2005); what influences information security behaviours (Leach, 2003) and, how attitudes and intentions are significant factors in explaining why some employees do not comply with information security policies (Pahnila et. al., 2007).

The study underway described in this paper adopts the model proposed by Stanton et. al (2005) in order to make conclusions about whether awareness training has an effect on specific behaviour categories. This model states that all security behaviour can be plotted on a behavioural continuum. On one level behaviour is categorised based on a user's intentions: from malicious to neutral to benevolent intentions. On another level behaviour can be categorized based on the level of expertise held by

the user ranging from novice to expert and something in between the two. This produces a two-factor taxonomy of user security behaviours yielding six broad behaviour categories as shown in figure 2 below.

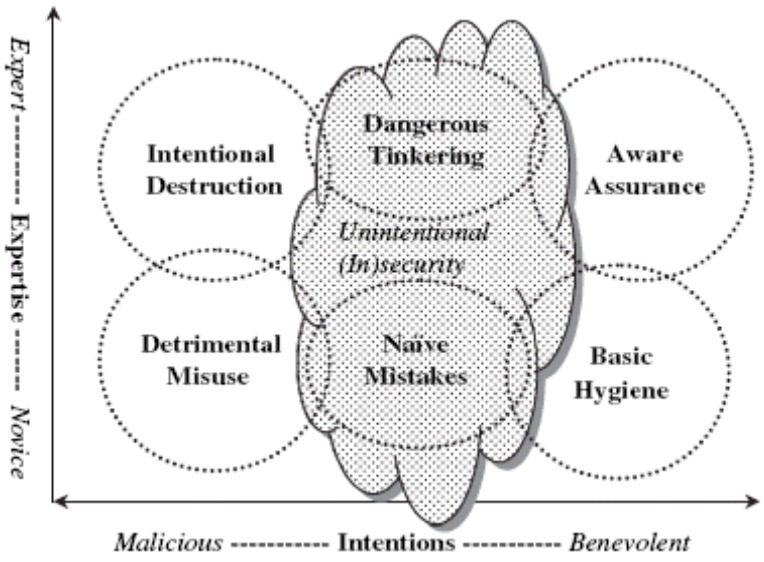

Figure 2. Two-factor taxonomy of end-user security behaviours (Stanton et. al 2005).

Using the model above, information security behaviours can be mapped against two-dimensions, i.e. the level of expertise the end-user possesses and the behavioural intent held by the end-user. The outcome is six different behavioural categories, which the researchers show, most security behaviours will be able to fit into (Stanton et. al, 2005:131). Putting this in context, the goal of security awareness initiatives is to move the intentions of employees towards the right-hand side of the chart. Thus Stanton et. al. (2005:132) provides a practical framework for categorising information security behaviours. This model now lays a foundation for the measurement of security behaviours. An illustrative example of the above taxonomy is shown in the table below:

Table 1.Examples of behaviours that that require low levels of expertise.

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

Stanton et. al. using simple correlation, showed that good password practices (such as changing passwords frequently and choosing strong passwords) was associated with training and awareness, employees' knowledge of being monitored and organisational benefits, perceived by employees (2005:124,131). A positive correlation does not mean that training and awareness caused these good password practices though. These password practices are known as naïve end-user security behaviours. These behaviours are characterised by individuals with a low level of expertise and with neutral intentions (neither malicious nor benevolent). Interestingly this same piece of research work did not find any correlation with another type of naïve security behaviour – that of sharing one's password. They concluded that there is no evidence that password sharing behaviour is associated with training, awareness, organisational rewards and knowledge of being monitored (Stanton et. al, 2005).

Additional research is needed in this area and is called for explicitly by Stanton et al. (2005). Secondly, different techniques will be used in the current study which may yield different results as those obtained from Stanton et. al. (2005). Vroom & von Solms (2004:191-192,194, 197) have also recognised the importance of human behaviour in the security chain but from an auditing perspective. The argument put forward is that although auditors express an opinion on an organisation's financial and IT arrangements, employee behaviour – which is a key aspect of information security - is not measured. They claim further that the reason that end-user behaviour is often neglected is because it is so difficult to measure and will inevitably be flawed. Auditing end-user behaviour is compared to carrying out employee performance appraisals and the resultant flaws associated with such activity namely: reliability and validity factors. They believe there are too many factors that may interfere with "auditing" the employee

accurately. Thus an alternative approach for auditing behaviour is put forward by them. They proposed that a better approach is to attempt to change organisational culture one level at a time and thereby influence end-user behaviour.

The implications of the Vroom & von Solms' work on this study are significant. Showing that behaviours can be measured in this context, adds a new dimension to the notion put forward by Vroom & von Solms. In addition, the techniques used and the lessons learned will form the groundwork for further research work to take place. Gaunt (2000:151,157), believes that information security awareness initiatives, while important, do not guarantee that staff will comply to appropriate security behaviours. Referring to the health care community he argues that a security culture needs to be entrenched for security to be effective. This requires amongst other things, strong commitment from senior management, clear lines of accountability and responsibility.

According to Gaunt's studies (2000:152-153), a number of obstacles need to be overcome to ensure security measures are effective and a culture of security is instilled. These include: Getting users to change their behaviour to a more secure form may be difficult especially if they have been used to using computer systems in an insecure way. Enforcing stronger security measures may in reality cause more reluctance by employees to change their behaviour. In addition to this, employees may view security measures as impractical and a hindrance to their work. Being unaware exactly what is required of them may also cause employees to become reluctant to embrace security.

Inconsistent application of policies among or within organisation's may lead to frustration by employees and thus undermine the effectiveness of the policies.

Gaunt research, while providing insight into obstacles, also indicates the complexity of the problem and its behavioural aspects. Pahnila et. al. (2007) demonstrate the complexity of security behaviour by arguing that compliance to policy is in fact made up of the intentions and attitudes of employees (which themselves are determined by various factors). They therefore recommend that promoting positive social pressure on employees with respect to compliance to security policies (for example, by all levels of management and peers within organisations) promotes actual security compliance. This should be done by explicitly stating what is required and,

by showing what needs to be done. This is inline with research carried out by Leach (2003). One of the factors that influence user security behaviour is what they are told. In most organisations this takes the form of security policies and security awareness initiatives (Leach, 2003:686). Another influencing factor in this regard is what employees see around them. Employees are strongly influenced by their peers and the messages that are released by the organisation whether internally or externally. If they see inconsistencies and contradictions between the message and the actual behaviour of the organisation, this will ultimately influence their behaviour (Leach, 2003:687).

4 THE NEED FOR FURTHER RESEARCH

According to Dhillon (1999), increasing awareness of security issues is the most cost-effective control that an organization can implement. Research that contributes to the effectiveness of awareness will ultimately benefit organisations as a whole as it will allow them to focus on techniques that improve their employees' intentions and ultimately encourage end-user security behaviours towards a more benevolent state. The research by Stanton et. al. (2005:132) implies that further research is needed in this respect as existing research does not address this appropriately. Diverse methods for measuring these different behaviours are also called for. This is needed since some behaviour may be easier to measure than others. Instruments that measure the behaviour of a database administrator (high technical expertise) that possesses malicious intent may be much more difficult than measuring behaviours that are more naïve in nature such as abuse of Internet access for example.

Kruger & Keaney (2005) developed a prototype for measuring the effectiveness of a security awareness program that was delivered in a global organisation. The model developed was based on three dimensions that could be measured i.e. what a person knows (knowledge), how they feel about a topic (attitude) and, what they do (a person's intention to act in a certain manner). These dimensions were measured to determine the effectiveness of their awareness programme. Information was gathered using questionnaires (including assessing behaviour) although they suggested using system data at a later stage. Thus actual behaviours of the employees were not measured to determine whether a difference was made. Kruger et. al. (2006) also recommends that system data be gathered to

supplement employee surveyed data and propose a basic list of source data from systems that could be used and for what purpose.

In some cases, researchers have however measured end-user behaviour directly, but this has been mainly geared towards how they respond to Internet-based threats, for example, the work carried out by Kumaraguru et. al. (2007), Jagatic et. al. (2007) and Whalen & Inkpen (2005). However the instruments used in these studies to measure certain behaviours may not be appropriate and practical for organisations to implement, such as those used by Whalen & Inkpen (2005). Learning science principles should be used (such as providing immediate feedback when incorrect behaviour is observed) and emphasis should be placed on the quality of awareness material as well as unique ways to deliver the message to end-users (Kumaraguru et.al., 2007). This is important since a lot is expected from users during awareness initiatives i.e. their time and attention, as well as expecting them to absorb the message. Srikwan & Jakobsson (2007), call for educational efforts to demonstrate and place emphasis on the link between behaviour and the outcome of that behaviour as they contend that mechanisms that support such a link "appears to offer significant benefits". Users must understand not only what they must do but why (Srikwan & Jakobsson, 2007:5).

The subject-expectancy effect, where a research subject expects a certain result, and therefore unconsciously affects the outcome of the results, are experienced by many surveys, such as the CSI survey mentioned above. Another example is the PayPal survey (PayPal, 2007) which provides a very good online questionnaire for users to test their understanding of phishing threats and how they work. Once again this type of survey however, does not measure actual behaviour.

Puhakainen (2006:69,139), points out that the only empirical evidence that does exist (with respect to information security awareness research) shows the practical effectiveness of deterrence. Further empirical evidence showing the effectiveness of security awareness training or awareness campaigns is not available, even though the effectiveness of training and campaign activities has been shown in other fields (for example, in cases where AIDS training has been a successful intervention).

Furthermore, scholars have pointed out that only a few existing studies are theoretically grounded (Puhakainen, 2006:149; Pahnila et. al. (2007)) and more work is needed in this regard. Security awareness research in this

context can be categorised as follows: conceptual models providing practical guidance for security awareness, theoretical models without empirical support and, theoretical models with empirical support (Pahnila et. al (2007)).

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

5 THEORETICAL UNDERPINNING

As mentioned above, a theory of security awareness is needed for researchers and practitioners to understand the expected outcomes of a particular awareness initiative and why this occurs. The model to explain security awareness training is based on work carried out by Nonaka & Takeuchi (1995). They argue that there are two types of knowledge and both are needed to help explain organisational learning, i.e. tacit knowledge and explicit knowledge. They propose that an organisation learns by oscillating between the two types of knowledge (Nonaka & Takeuchi, 1995:61). Tacit knowledge is not tangible and is subjective since it is that which is possessed by employees of the organisation. This includes individual beliefs, experiences and understandings of the organisation and what the organisation requires from them. Explicit knowledge on the other hand is codified, formal and easily expressed. Examples of this are organisational policies and pamphlets. Nonaka & Takeuchi (1995:70, 71) argue that the learning path in an organisation follows four cyclical stages:

- Employees share tacit knowledge;
- Tacit knowledge is made explicit by formalising it (e.g. policies);
- Formalised knowledge is disseminated (e.g. awareness activities) and,
- Employees “learn by doing” and thus explicit knowledge is made tacit by employees internalising it.

The cycle then starts from stage 1 again and follows an infinite loop. The study in progress described in this paper proposes a theoretical model to help explain how awareness training influences behaviour. The study in progress aims to show that in order to ensure appropriate security behaviour, employees need explicit knowledge of security policies and tacit knowledge on how to enact the appropriate security behaviour.

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

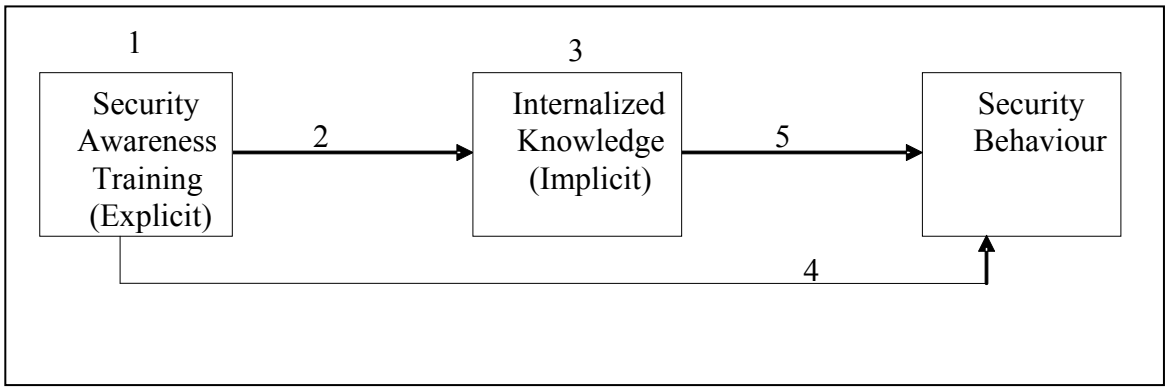

Figure 3. Theoretical model explaining how security awareness training affects behaviour.

6 RESEARCH AGENDA AND IMPLICATIONS

The previous section presents a theoretical model explaining how the authors expect security awareness training to affect behaviour. This section will put forward a research agenda for scholars and practitioners to explore further.

Security awareness training should influence all employees within an organisation to ensure the appropriate behaviour is enacted by all and thereby achieve compliance to information security policies. To confirm this, the following questions should be further explored: In terms of explicit knowledge, what type of security awareness training is more likely to influence behaviour i.e. how important is the quality of the awareness material and the mechanism of delivery? How could practitioners more easily deliver the awareness message to ensure greater participation from end-users? Standardised, cost-effective and automated mechanisms for gathering system generated data (especially for behaviours requiring high levels of expertise) and the feasibility of such mechanisms require additional investigation. In terms of implicit knowledge, further standardised mechanisms should be explored to determine how best to measure implicit knowledge taking into account the role of learning science principles. What are the most effective learning principles and under what conditions are they effective? Status of employees within the organisation and the role that plays in awareness training is important to determine in future research. Once users fully comprehend policies, are the same types of interventions necessary to sustain the required behaviours? This is important as it will likely determine how often awareness interventions are required. Longitudinal studies in this regard would be necessary. An understanding of the influence of factors such as user attitude, perceptions and corporate politics on internalisation of the security awareness message and subsequent behaviour is also needed. Finally, further research is needed on a taxonomy of security behaviours, building on the work of Stanton et. al. (2005).

The implications for practitioners are potentially significant. In order for organisations to implement affective Information Security an understanding from all employees within an organisation is needed. In addition, compliance to these policies is necessary and in some cases needs to be demonstrated by the Information Security function or Risk Management function within an organisation to justify their activities. The outcome of the current study will potentially provide pragmatic guidance for practitioners

when designing and implementing their information security awareness programmes.

7 CONCLUSION

There is a shortage of research on behavioural information security and theoretical models explaining how awareness training affects behaviour. The study in progress builds on existing behavioural information security research and puts forward a theoretical model, based on an organisational learning model. This theoretical model explains how organisational learning takes place, showing that both explicit knowledge and implicit knowledge is needed. The research underway will test the proposed model using system-generated data as indicators of behaviour in a pretest-posttest experimental design. Only a subset of behaviours (based on a typical Acceptable Usage Policy) that require low technical expertise on the part of the end-user will be tested. The objective of this research is to determine the effectiveness of information security awareness training on subsequent behaviour by users in the study. Such a model could help scholars and practitioners understand why an awareness initiative is expected to have certain results on security behaviour and consequently, provide practitioners with practical guidance for their information security programmes.

8 REFERENCES

Computer Security Institute (CSI). 2006. Virus Attacks Named Leading Culprit of Financial Loss by U.S. Companies in 2006 CSI/FBI Computer Crime and Security Survey [online]. [Accessed 9th August 2006]. Available from World Wide Web: <http://www.gocsi.com/press/20060712.jhtml>

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

Dhillon, G. 1999. Managing and controlling computer misuse. Information Management & Computer Security, Vol. 7, Issue 4, pp/ 171-175.

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

Furnell, S., Sanders, PW., Warren, MJ. Addressing IS security training and awareness within the European healthcare community. In Proceedings of Medical Informatics Europe '97. 1997.

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

Furnell, SM., Why users cannot use security. Computers & Security 24,

4, 2005, 274-279.

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

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

Jagatic, TN., Johnson, M., Jakobsson, M., Menczer, F. Social Phishing.

Communications of the ACM. Vol. 50, Issue 10, 2007, pp. 96 – 100.

Janczewski L, Xinli Shi F. 2002. Development of Information Security Baselines for Healthcare Information Systems in New Zealand. Computers & Security, Vol. 21, No. 2, pp 172 – 192.

Johnston, J., Eloff, JHP., Labuschagne, L. Security and human computer interfaces. Computers & Security, Volume 22, Issue 8, December 2003, Pages 675-684.

Katsikas SK. 2000. Health care management and information systems security: awareness, training or education? International Journal of Medical Informatics, Vol. 60, pp 129-135.

Kruger HA, Drevin L, Steyn T. A framework for evaluating ICT security awareness. Proceedings of the ISSA 2006 from Insight to Foresight Conference 5 July – 7 July 2006, Balalaika Hotel, Sandton, South Africa.

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

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., Nunge, E., Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. Conference on Human Factors in Computing Systems archive. Proceedings of the SIGCHI conference on Human factors in computing systems. San Jose, California, USA, 2007, pp. 905 – 914.

Leach J. 2003. Improving user security behaviour. Computers & Security, Vol. 22, No. 8, pp 685-692.

McCoy, C., Fowler, RT. You are the key to security: establishing a successful security awareness program. In the proceedings of the SIGUCCS'04, Baltimore, Maryland, October 10-13, 2004, pp. 346-349.

Mitnick, KD., Simon WL., 2002. The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons.

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

Nonaka, I, Takeuchi H. (1995), The Knowledge Creating Company, New York: Oxford University Press.

Nosworthy JD. 2000. Implementing Information Security In The 21st Century – Do You Have the Balancing Factors? Computers & Security, Vol. 19, pp 337 – 347.

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

Parker, DB. 1998. Fighting Computer Crime: A new Framework for Protecting Information. USA: John Wiley & Sons.

Pahnila, S., Siponen, M., Mahmood, A. Employees' Behavior towards IS Security Policy Compliance. Proceedings of the 40th Hawaii International Conference on System Sciences, 2007.

PayPal. 2007 [online]. Can you spot phishing [Accessed 2008]. Available from World Wide Web: <https://www.paypal.com/fightphishing >

Perry, WE. 1985. Management Strategies for Computer Security. USA:

Butterworth Publishers.

Puhakainen, P. 2006. *A Design theory for Information Security Awareness.* Ph.D. thesis, University of Oulu.

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

Schneier B. (2003), Beyond Fear, Copernicus Books, New York

Schneier B. (2000), Secrets & Lies, Wiley Computer Publishing, New York

Schultz E. Security training and awareness—fitting a square peg in a round hole. Computers & Security, Vol. 23, Issue 1, 2001, pp 1 – 2.

Siponen MT. A conceptual foundation for organizational information security awareness. Information Management & Computer Security, Vol. 8, Issue 1, 2000, pp. 31-41.

Siponen, MT. 2001. Five dimensions of Information Security Awareness. Computers and Society, Vol. 32, Issue 2, 2001, pp 24-29.

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

Spurling, P., "Promoting security awareness and commitment", Information Management & Computer Security, 3, 2, 1995, 20-26.

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

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

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

Thomson ME, von Solms R. Information Security Awareness: Educating your users effectively. Information Management & Computer Security, Vol. 6, Issue 4, 1998, 167-173.

Trompeter, CM., Eloff, JHP. A framework for the implementation of socio-ethical controls in information security. Computers & Security, Vol. 20, 2001, pp 384-391.

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

Von Solms B. Information Security – The Third Wave. Computers & Security, Vol. 19, 2000, pp 615 – 620.

Von Solms B. Information Security - A multidimensional Discipline. Computers & Security, Vol. 20, 2001, pp 504 – 508.

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

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