CONF-IRM 2016 Proceedings

International Conference on Information Resources Management (CONF-IRM)

2016

Towards using pervasive information security education to influence information security behaviour in undergraduate computing graduates

Thandolwethu Mabece
Nelson Mandela Metropolitan University, s20802053@nmmu.ac.za

Lynn Futcher
Nelson Mandela Metropolitan University, lynn.futcher@nmmu.ac.za

Kerry-Lynn Thomson
Nelson Mandela Metropolitan University, kerry-lynn.thomson@nmmu.ac.za

75. Towards using pervasive information security education to influence information security behaviour in undergraduate computing graduates

Thandolwethu Mabece
Nelson Mandela Metropolitan University,
s20802053@nmmu.ac.za

Lynn Futcher
Nelson Mandela Metropolitan University
Lynn.Futcher@nmmu.ac.za

Kerry-Lynn Thomson
Nelson Mandela Metropolitan University
Kerry-Lynn.Thomson@nmmu.ac.za

Abstract

Information security has become increasingly important and is far more than a collection of physical and technical controls. It is widely cited in literature that humans are potentially the 'weakest link' when it comes to information security, whether intentionally or unintentionally. For information security to be truly effective, the behaviour and actions of users, with regard to information security, should become part of their daily activities and, ultimately, part of an information security culture. Therefore, it could be argued that graduates entering the employment of an organisation should be aware and properly educated with regard to information security and its related practices. This information security awareness and education should, preferably, be a part of their formalized studies. This is particularly important for those graduates with computing qualifications as they could play a vital role in ensuring the protection of an organisation's information assets. This paper motivates the need for the implementation of pervasive information security education in computing undergraduate curricula, which could positively influence the information security behaviour of computing graduates. This research is based on a literature study.

Keywords

Information security awareness, information security education, information security culture, information security behaviour.

1. Introduction

Users often participate in risky behaviour that can threaten the confidentiality, integrity and the availability of information assets. User behaviour accounts for the majority of security breaches experienced by organisations, although often not with malicious intent to cause harm. Users who have not been educated with regard to information security could be easy targets for hackers because of their ignorance. Therefore, educated and trained people could be a critical success factor in order to mitigate threats within organisations (Al Awawdeh & Tubaishat, 2014; Cox, 2012).

Once graduates leave higher education institutions, it is very likely that they will become employees in organisations. It is important that these graduates stay abreast of industry changes, as these graduates need to be able to solve real world problems. If the university curriculum does not offer the necessary tools needed to solve these real world problems, then the university has failed (Lunt et al., 2008). With regard to computing graduates, it is vital that these graduates are aware of and are educated about the importance of information security and that they have the necessary skills and behaviour to protect information assets. In the context of this research, computing graduates refer to Information Technology (IT), Information Systems (IS) and Computer Science (CS) graduates.

The Association for Computing Machinery (ACM) curricula guidelines (ACM, 2013) describe what characteristics computing graduates should have when they have completed their degrees. The IT guidelines specifically state that an IT graduate should have an "*understanding of professional, ethical, legal,* ***security*** *and social issues and responsibilities".* The CS guidelines explain that a graduate "*needs a set of general principles, such as sharing a common resource,* ***security,*** *and concurrency"* (ACM, 2013). This, therefore, suggests that graduates from these disciplines should be information security conscious, particularly when they move into organisations. These computing graduates should contribute to the much needed information security conscious workforce, and could be the champions of information security initiatives within organisations.

Higher education institutions are responsible for producing computing graduates who understand and execute information security initiatives. These graduates are also required to meet the needs of industry when employed by organisations (Talib, Khelifi, & Ugurlu, 2012). International standards and guidelines provide guidance for security requirements within organisations and to fulfil these requirements organisations need employees with the necessary knowledge and skills to help alleviate security breaches (Armstrong, 2011; Talib et al., 2012). It is important that computing graduates demonstrate the correct information security behaviour to be able to solve these real world security-related problems.

This paper argues that a need exists for the implementation of pervasive information security education in undergraduate computing curricula in order to influence the graduates' information security behaviour. Pervasive, in this context, is defined as "*existing in all parts of a place or thing; spreading gradually to affect all parts of a place or thing*" (Oxford Dictionaries, 2015). Section 2 addresses information security within organisations, while Section 3 highlights the current state of information security in undergraduate computing curricula. Section 4 considers information security behaviour, followed by a discussion on information security culture in Section 5. Section 6 explores the proposed solution to this research and finally the paper concludes with Section 7.

2. Information security in organisations

The importance of information being a vital business asset cannot be stressed enough. Information is critical to organisations. However, it is vulnerable to various threats and attacks from both insiders and outsiders. Insider threats may cause more damaging and costly incidents than outsider threats. Despite organisations taking various technical countermeasures to protect these assets, information security breaches are still increasing rapidly. This is possibly due to a lack of cooperation from users or a lack of knowledge on how to implement relevant controls. Organisations therefore need to focus their attention more on their users in order to mitigate potential threats, as it is often said that users are the greatest threat to information security (Tajuddin, Olphert, & Doherty, 2014; Tu & Yuan, 2014; PricewaterhouseCoopers, 2014).

Further, organisations should have information security policies in place to communicate to users what the acceptable information security behaviour is. User compliance with regard to these policies is essential in ensuring that information assets remain protected. However, users often ignore, or do not comply with these policies for various reasons, for example, a lack of awareness and ignorance (Cox, 2012).

Van Niekerk and von Solms (2005) argue that many security controls are liable to be misused or misinterpreted by users who do not have adequate security knowledge. Users have to be educated and trained to be information security conscious and motivated to comply with security policies and procedures. Education is important to not only teach users what to do and how to do it, but also why it should be done (van Niekerk & von Solms, 2005). According to Schein (1999), users will often refuse to accept the need for new, responsible behaviour patterns until they have been educated about a particular topic. An example of such topics would be threats to information assets and the need for information security. Education is often the only way to convince users of the need to do things differently (Schein, 1999). Therefore, users who are educated regarding information security best practices could be the strongest link within an organisation when it comes to the protection of information assets. This could assist in the mitigation of some of the threats (Al Awawdeh & Tubaishat, 2014; Chen, Ramamurthy, & Wen, 2015).

Within the context of this paper, higher education institutions are organisations. Additionally, within the context of this paper, it is important to create the correct information security culture within higher education institutions. When computing graduates are employed in organisations, they too become users. Therefore, it could be argued that if computing graduates have been exposed to information security education during their studies, they could champion information security initiatives within these organisations. The following section explores information security in computing curricula.

3. Information security in computing curricula

Information security education should be offered at undergraduate, graduate and postgraduate levels at all academic institutions to cope with the prevailing information security problems plaguing organisations (Hentea, Dhillon, & Dhillon, 2006). Computing graduates entering the work environment should be able to exhibit and be skilled in the underlying principles of information security (Futcher, Schroder, & von Solms, 2010). These graduates would, for example, typically be computer programmers, information security analysts, software developers, and database administrators. As such, they would interact with information assets and information systems. Information security education should, therefore, teach these students the fundamental principles they need in order to preserve and protect the confidentiality, integrity and availability of an organisation’s information assets (Florentine, 2014; Pratt, 2014).

According to the ACM, Information Assurance and Security (IAS) should be a very important part of computing curricula. IAS is defined as "*a set of controls and processes, both technical and policy, intended to protect and defend information and information systems by ensuring their confidentiality, integrity, and availability, and by providing for authentication and non-repudiation*". Assurance ensures that these processes and information are valid, while security ensures that these processes and information are protected (Committee on National Security Systems, 2010).

The ACM guidelines for both IT and CS describe IAS as an integrative knowledge area that should be pervasive throughout other knowledge areas. However, the ACM IT guidelines state that IAS belongs at the advanced level of a four year IT program. Yet, some students do not get the chance to complete a fourth year of study. Therefore, it could be argued that these students may never encounter IAS education in other words information security education. The ACM IS guidelines refer to IAS as IT security and risk management; it also states that this is an elective course. More emphasis should be placed on this knowledge area to ensure that it permeates undergraduate programs; not as a standalone course, but rather as a "*pervasive"* theme in order to cultivate an information security conscious workforce in the future (ACM, 2013; Lunt et al., 2008; Topi et al., 2010). Therefore, for information security to become pervasive, relevant topics could be taught, to some extent, in all of the modules of the main curriculum from first year through to the final year (Lunt, et al., 2008). In addition, core security skills should be identified and pervasively integrated into undergraduate computing curricula. This does not mean that each individual module needs to handle all the core security skills; however, each module should incorporate those most relevant through examples, scenarios and topics.

Higher education institutions have made advances in implementing information security in postgraduate programs; however, there is still a need for a pervasive information security program in undergraduate computing curricula (Futcher et al., 2010). Information security education is necessary in ensuring that users have the required knowledge to behave in a secure manner and, users often need to be educated in order for them to be convinced to demonstrate new behaviour patterns (Okere, van Niekerk, & Carroll, 2012; Schein, 1999). The following section discusses information security behaviour.

4. Information security behaviour

There is general consensus in literature that user behaviour poses significant risk in the protection of information assets. It is also acknowledged, however, that if users behave in a secure manner, this could lead to the successful protection of information assets (Alhogail & Mirza, 2014a; Thomson & von Solms, 2006; van Niekerk & von Solms, 2010). Although organisations invest a great deal in new technology in an effort to try and protect their information assets, this is not enough. Organisations need to focus more on user behaviour and find ways in which they can positively influence this behaviour to ensure that information security becomes second nature to their employees (Blythe, 2013). As mentioned previously, higher education institutions can be regarded as organisations and therefore the same information security concepts or principles would apply.

The behaviour of users is critical in ensuring the protection of information assets. The focus of this research is primarily the behaviour of computing graduates regarding information security practices. It is, therefore, necessary to consider theories that deal with behaviour (van Niekerk, 2005). One such theory is Ajzen's Theory of Planned Behaviour which helps to understand how to change the behaviour of people. As the name suggests, this theory helps predict deliberate behaviour of people because behaviour can be planned (Ajzen, 1991). Figure 1 illustrates the Theory of Planned Behaviour elements that contribute to the behaviour of people.

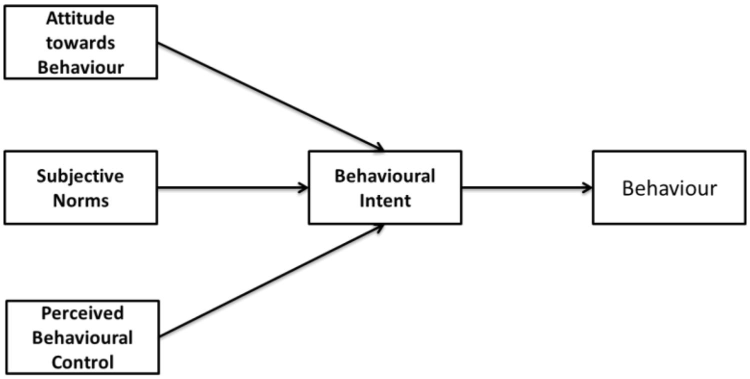

Figure 1-The Theory of Planned Behaviour
(Ajzen, 1991)

According to the theory, *attitudes*, *subjective norms* and *perceived behavioural control* all influence a person's *behavioural intent* which ultimately determines their *behaviour*. *Attitude* is concerned with the person's feelings and beliefs (Ajzen, 1991). The possibility of a person adhering to the correct behaviour is greater with a positive attitude. If users have a positive attitude towards information security, they are more likely to comply with the correct behaviour. *Subjective norms* are perceptions and expectations that the person has about the people and environment around them, for example, social groups (Ajzen, 1991). If the social group around a user is accepting of information security best practices, then the user will most likely be influenced to perceive information security in the same light. *Perceived behavioural control* is concerned with the perceived capability of an individual to execute the required behavioural change. Furthermore, it includes an individual's confidence in performing that behaviour (Ajzen, 1991). Education could be used to specifically address the *perceived behavioural control*. For example, if a user is given the correct skills and tools through education, they could feel more confident in altering their behaviour to the required information security behaviour. *Behavioural intent* represents the person's willingness to achieve the required behaviour influenced by *attitude*, *subjective norms* and *perceived behavioural control* (Ajzen, 1991). In the context of information security, if all three elements that influence *behavioural intent* are favourable, the intention towards behavioural change with regards to information security will be stronger.

5. Information security culture

Humans are potentially the "weakest link" when it comes to information security, whether intentionally or unintentionally. Protecting information should become second nature to all users. Therefore, for information security to be effective, an information security culture should ideally exist (van Niekerk & von Solms, 2004; von Solms & von Solms, 2004).

Schein (1999) defines culture as "*a pattern of shared basic assumptions learned by a group as it solves its problems of external adaptation and internal integration, which has worked well* *enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems*". This definition highlights two important factors. Firstly, shared basic assumptions need to be defined as the "working solution" to specific problems or challenges. Secondly, these shared basic assumptions need to be taught to new users as the acceptable behaviour.

Information security culture forms part of the overarching organisational culture. Within the context of this paper, higher education institutions are organisations. Organisational culture, therefore, influences information security culture (Thomson & von Solms, 2005). The presence of a strong information security culture could possibly influence the information security behaviour of employees (Alhogail & Mirza, 2014). According to Hu et al.(2012), information security culture shapes and guides the information security behaviour. Similarly, an organisation's information security culture is cultivated by the information security behaviour of its users (Da Veiga & Eloff, 2010). If an information security culture does not exist within an organisation, the behaviour of new employees, for example computing graduates, coming into the organisation could influence the cultivation of an information security conscious culture (van Niekerk & von Solms, 2005; von Solms & von Solms, 2004b).

There are a number of ways in which an information security culture could be cultivated. This would include, for example, education and influencing the behaviour of users. Education deals with teaching users about the importance of information security, their roles and responsibilities and why these roles exist. Behaviour is concerned with the attitudes, perceptions and intention of users with regard to conforming to the required behaviour (Schein, 1999). For the purposes of this paper, the focus is on information security behaviour of computing graduates within higher education institutions.

Von Solms and von Solms (2004a) claim that to ensure that the behaviour and actions of users are aligned with management's vision for the organisation, an appropriate information security culture should be cultivated. Information security culture is defined as "*the collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in an organisation with the aim of influencing employees' security behaviour to preserve information security"* (Alhogail & Mirza, 2014). This definition can be likened to the Theory of Planned Behaviour which deals with *attitudes*, *subjective norms* and *perceived behavioural control*, which ultimately influence behaviour. Therefore, the more evident the information security culture is within higher education institutions, the more likely computing graduates will exhibit compliant security behaviour.

A positive information security culture is essential as it is the driving force that reinforces individual and group behaviour. Positive user behaviour or compliant behaviour could help mitigate threats to information systems (Alhogail, 2015; Brien et al., 2013; Guo, 2013). A robust information security culture may alleviate many of the users' behavioural issues that cause information security breaches (Alhogail & Mirza, 2014).

6. Addressing the "weakest link"

An information security culture could play an integral role in the protection of information assets by addressing humans as the 'weakest link'. However, such a culture requires users who exhibit acceptable information security behaviour. Behaviour can be influenced by a number of factors such as awareness and education. Lack of knowledge, negative behaviour and lack of commitment from users are the biggest concerns when it comes to the protection of information assets (van Niekerk & von Solms, 2005). However, knowledgeable or educated users could be the strongest link within organisations. In the context of higher education institutions, these users could be computing graduates. In order for an individual to become knowledgeable or educated about something, knowledge creation must take place.

Nonaka (1994) highlights two dimensions of knowledge creation: *explicit* and *tacit* knowledge. Explicit knowledge is objective and it can be expressed in words, for example, policies in computing laboratories and curricula. Conversely, tacit knowledge is subjective and is difficult to formalize and communicate. It is rooted in action, commitment and involvement. Tacit knowledge is comprised of, for example, beliefs, assumptions, norms, attitudes as well as skills. There are four identified modes of the relationships between explicit and tacit knowledge that are referred to as Nonaka's Modes of Knowledge Creation.

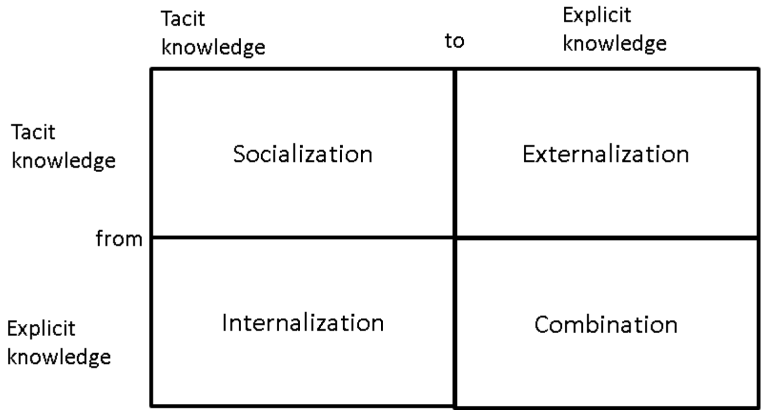

Figure 2- Modes of Knowledge Creation
(Nonaka, 1994)

Figure 2 illustrates the Modes of Knowledge Creation which include *Externalization, Combination, Internalization, and Socialization* (Nonaka, 1994). *Externalization* is the conversion of tacit knowledge into explicit knowledge. This means that the beliefs and principles are expressed verbally or in written form. Externalization can be articulated through dialogue between individuals or through policies (Nonaka, 1994). *Combination* is the process of transferring explicit knowledge to explicit knowledge. This means that knowledge can be transferred between groups. Explicit knowledge can be communicated, for example, through policies, posters, emails, and presentations (Nonaka, 1994). Education would specifically be used as a form of combination. *Internalization* transforms explicit knowledge into tacit knowledge. For example, values and beliefs explicitly expressed in policies, which the individual has to comprehend and comply with, are converted into the individual's tacit knowledge (Nonaka, 1994). *Socialization* is the mode where tacit knowledge is converted into tacit knowledge via the interaction of individuals. Socialisation is the result of non-verbal communication and interaction of individuals. An individual can absorb another individual's tacit knowledge through observation and practice without articulating verbally. Experience is vital to obtaining tacit knowledge (Nonaka, 1994). According to the ACM guidelines, the core security knowledge that students need to be taught include, for example an understanding of security threats, vulnerabilities, legal and ethical aspects of information security and password security. Students are taught these core security topics in multiple classes through practicals, lectures and tutorials. This is the *combination* mode. During these practicals, lectures and exams, students internalise these core security topics. Through the interaction of students and educators, *socialisation* takes place.

It is important for computing graduates to exhibit the correct information security behaviour, which may ultimately influence the information security culture both within the higher education institutions, as well as in their future working environments. Figure 3 depicts how to potentially influence the behaviour of computing graduates.

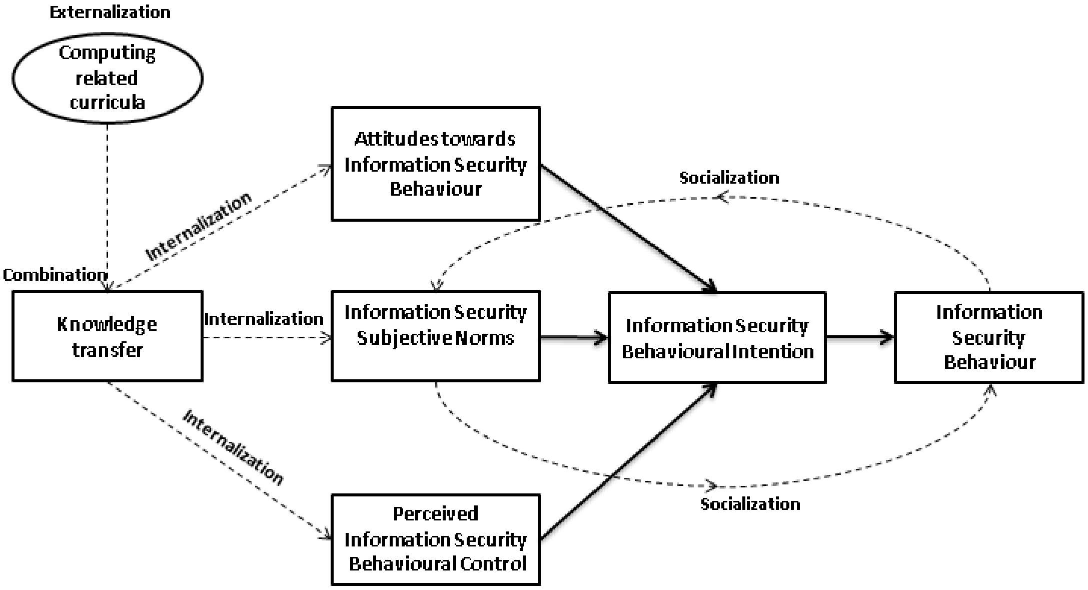
Externalization
Computing related curricula
Attitudes towards Information Security Behaviour
Socialization
Internalization
Combination
Knowledge transfer
Internalization
Information Security Subjective Norms
Information Security Behavioural Intention
Information Security Behaviour
Internalization
Socialization
Perceived Information Security Behavioural Control

Figure 3- Influencing the information security behaviour of computing graduates.

Figure 3 represents the aspects of an individual's behaviour, and the influences, both internal and external, that need to be considered in order to possibly change the individual's behaviour. *Externalization* mode is the starting point in this diagram. It could be argued that computing curricula guidelines are required to explicitly explain how information security should be implemented as a pervasive theme in all computing curricula and indicate what should be taught. If people do not know how to behave with regards to information security, they cannot be expected to exude the required behaviour. As mentioned previously, externalization is the process of converting tacit knowledge into explicit knowledge. In Figure 3 the tacit knowledge of the authors of the ACM curricula guidelines is, for example, externalised into the various computing curricula. *Combination* occurs when explicit knowledge is transferred into explicit knowledge. This process happens when the students are taught in the classrooms or when they implement information security practices practically. *Internalization* is the transfer of explicit knowledge to tacit knowledge. When a student has learnt the information security practices (through combination), they should internalise that knowledge which then influences their attitudes, subjective norms and their perceived behavioural control. Their attitudes towards the required information security behaviour can be positive or negative. Subjective norms of an individual are influenced by the perceptions of what those around them think. If their social norms deem the required information security behaviour to be good, there is a greater chance that the individual may be persuaded to change their behaviour. Conversely, if the individual's environment is not conducive to the correct information security behaviour, then the chances that the individual will change their behaviour is less likely. Further, the more an individual feels confident to perform the necessary information security behaviour, known as perceived behavioural control, the greater their chance of actually conforming to that behaviour. This all forms part of the internalisation process. *Socialization* happens when tacit knowledge is transferred into tacit knowledge. As the name suggests, it is an on-going social process where individual knowledge is transferred by way of interaction, non-verbal communication and observation.

So once the student has acquired the correct information security knowledge and they interact with other students and educators who demonstrate the required information security behaviour, this has the potential to influence the student to also demonstrate the required information security behaviour.

An example could be that of user knowledge and behaviour relating to password security that would be important for computing graduates. This topic would need to be included in the curricula guidelines representing the tacit knowledge that has been externalised into explicit knowledge. This is the externalization process. These password security guidelines would then be transferred into the explicit knowledge of the students when they are taught in various classes. This is where the pervasiveness of information security throughout computing curricula is imperative. The topic of password security would not only be taught in a security related subject, but would be emphasised in multiple modules as being significant. This explicit password security knowledge could include the importance of password security; how to create strong passwords and how to protect the password, for example. This process is referred to as the combination process. The students then internalise this explicit knowledge into tacit knowledge through practical experience. In their practical classes, they could practice how to set up a good password. With enough practice, password protection could become second nature to these students. This knowledge could influence the attitudes and perceived behavioural control of the students. However, the subjective norms, which relate to the environment, would require that measures are in place, for example, in the computer laboratories to ensure adherence to password security best practices. The subjective norms, together with the attitudes and perceived behavioural control of the students will ultimately influence their behaviour regarding password security. With the socialization of students and educators, the process of tacit knowledge being transferred into tacit knowledge occurs. Students would observe and mimic how their educators and peers behave with regards to password security. Information security education is fundamental in influencing the behaviour of users. It is essential in ensuring that users have the necessary knowledge to behave in a safe manner. If users have the required information security knowledge, it could positively influence their information security behaviour. Ultimately, an ideal environment would be one where the protection of information assets is second nature to users.

7. Conclusion

For computing graduates the necessary information security knowledge should, ideally, be imparted in their undergraduate computing curricula as part of their studies. However, for information security knowledge and practices to become part of the behaviour of computing graduates, it is argued that an isolated information security related module is not sufficient. This paper proposes that information security topics should be pervasively integrated throughout undergraduate computing modules in an attempt to influence the *perceived behavioural control*, *attitudes* and *subjective norms* of computing graduates. This would have an impact on the *behavioural intent* of computing graduates and, ultimately, positively influence the information security *behaviour* of these computing graduates. When these graduates become employees in the workplace, they could positively influence the information security culture of the organisation.

8. Acknowledgements

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

References

ACM. (2013). Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science. Practice (pp. 1–172).

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

Al Awawdeh, S., & Tubaishat, A. (2014). An information security awareness program to address common security concerns in IT unit. *ITNG 2014 - Proceedings of the 11th International Conference on Information Technology: New Generations*, 273–278.

Alhogail, A., & Mirza, A. (2014). Information security culture: a definition and a literature review. In *Conference proceedings of IEEE World Congress On Computer Applications and Information Systems*. IEEE computer society.

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575.

Blythe, J. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. In *Proceedings of CHItaly 2013 Doctoral Consortium* (pp. 92–101). Chieti: Springer. Retrieved from http://ceur-ws.org/Vol-1065/paper11.pdf

Brien, J. O., Islam, S., Bao, S., Weng, F., Xiong, W., & MA, A. (2013). Information security culture: Literature Review. *The University of Melbourne Library*.

Chen, Y. A. N., Ramamurthy, K. R. A. M., & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11–19.

Committee on National Security Systems. (2010). *National Information Assurance (IA) Glossary*. *CNSS Instruction*.

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

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207.

Florentine, S. (2014). Top 10 IT Skills Based on Increases in Demand. Retrieved August 14, 2015, from http://www.cio.com/article/2832678/it-skills/165725-Top-10-IT-Skills-Based-on-Increases-in-Demand.html#slide11

Futcher, L., Schroder, C., & von Solms, R. (2010). Information security education in South Africa. *Information Management & Computer Security*, *18*, 366–374.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*(1), 242–251.

Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education*, *5*, 221–233.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences*, *43*(4), 615–660.

Lunt, B. M., Ekstrom, J. J., Gorka, S., Hislop, G., Kamali, R., Lawson, E., … (Chair), B. M. L. (2008). *Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology*. *ACM* (pp. 1–139).

Nonaka, I. (1994). A Dynamic Theory of Organizational Knowledge Creation. *Organization Science*, *5*(1), 14–37.

Okere, I., van Niekerk, J., & Carroll, M. (2012). Assessing Information Security Culture: A Critical Analysis of Current Approaches. *Information Security for South Africa (ISSA)*, *2012*, 1–8.

Oxford Dictionaries. (2015). Oxford Dictionaries- Language matters. Retrieved May 01, 2015, from http://www.oxforddictionaries.com/definition/learner/pervasive

Pratt, M. K. (2014). 10 hottest IT skills for 2015. Retrieved August 14, 2015, from http://www.computerworld.com/article/2844020/it-careers/10-hottest-it-skills-for-2015.html

PricewaterhouseCoopers. (2014). Global State of Information Security Survey: Key findings and trends. Retrieved July 30, 2015, from http://www.pwc.com/gx/en/consulting-services/information-security-survey/key-findings.jhtml

Schein, E. . (1999). *The corporate culture survival guide:Sense and nonsense about culture change*. San Francisco, Calif.: Jossey-Bass.

Tajuddin, S., Olphert, W., & Doherty, N. F. (2014). Relationship between stakeholders' information value perception and information security behaviour. In *AIP conference Proceeding*.

Talib, M. A., Khelifi, A., & Ugurlu, T. (2012). Using ISO 27001 in teaching information security. In *IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society* (pp. 3149–3153). Montreal, QC: IEEE.

Thomson, K-L., & von Solms, R. (2005). Information security obedience: A definition. *Computers and Security*, *24,* 69–75.

Thomson, K-L., & von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud and Security*, *2006*(May), 11–15.

Topi, H., Valacich, J. S., Wright, R. T., Kaiser, K., Nunamaker, J. F., Sipior, J. C., & de Vreede, G. J. (2010). *IS 2010: Curriculum guidelines for undergraduate degree programs in information systems*. *Communications of the Association for Information Systems* (Vol. 26, pp. 359–428).

Tu, Z., & Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management : A Literature Review. *Information Systems Security, Assurance, and Privacy Track (SIGSEC)*, 1–13.

Van Niekerk, J. (2005). Establishing an Information Security Culture in Organizations: an Outcomes Based Education Approach.

Van Niekerk, J., & von Solms, R. (2010). Information security culture: A management perspective. *Computers and Security*, *29*(4), 476–486.

Van Niekerk, J., & von Solms, R. (2004). Organisational learning models for information security. *The ISSA 2004 Enabling Tomorrow Conference*, *30*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?

Van Niekerk, J., & von Solms, R. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. *Issa*, 1–13.

Von Solms, B., & von Solms, R. (2004a). The 10 deadly sins of information security management. *Computers and Security*, *23,* 371–376.

Von Solms, R., & von Solms, B. (2004b). From policies to culture. *Computers and Security*, *23*, 275–279.