Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

A Comprehensive Framework for Cultivating and Assessing Information Security Culture

A. Tolah[1], S.M. Furnell[1,2,3] and M. Papadaki[1]

[1] Centre for Security, Communications and Network Research, University of Plymouth, UK
[2] Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, South Africa
[3] Security Research Institute, Edith Cowan University, Western Australia
e-mail: {alaa.tolah, steven.furnell, maria.papadaki }@plymouth.ac.uk

Abstract

The efficiency of different technical security controls is based on people who interact with the information daily. An understanding of human behavioural aspects is required in order to improve the security of information assets. One of the measures that can be used as a way to reduce risks posed by a human is by establishing an information security culture that aims to protect information by guiding organisations on how to protect assets, as well as exerting an influence upon the employee's behaviour regarding the security. Previous analyses have concluded that an understanding of the information security culture and its measurements are still lacking. Specifically, more research needs to provide a comprehensive view that guides and integrates the important factors that shape, or have an impact on, the information security culture. Furthermore, there are efficient factors that were widely investigated in the organisational behaviour literature and can motivate employee behaviour toward the information security. These factors have not been deeply considered in the information security culture field. In this paper, a comprehensive literature analysis relating to the information security culture is conducted. This study proposes an initial information security culture framework by considering the identified human factors that can be used to measure the level of the information security culture and assist researchers and practitioners to understand the complexity and challenges of the information security culture.

Keywords

Information security culture (ISC), insider threat, human factor.

1. Introduction

Over the years, various technical approaches have been developed in relation to security and different countermeasures. However, there has been an acceleration of breaches that unfortunately create added pressures to the professionals working within IT. A greater level of vulnerable components in information systems exist nowadays from the individuals who use the information technology (Information Security Breaches Survey, 2015). Several studies indicated that information security can no longer be achieved by technological issues alone, as it is also associated with personal issues who actually operate these systems (Connolly et al. 2017).

It was indicated that technology was less likely to cause problems than a human error, which is a cause of the majority of breaches in security, as 75% of organisations were revealed to suffer security breaches by insiders (Information Security Breaches Survey, 2015). Indeed, many studies examined the human factor and its relation to an information security with the social psychology issues, which determine the reason behind unacceptable behaviour that leads to breaches (Parsons et al. 2017). It was stated that one approach that organisations can take to manage the changing security landscape would be to develop strategies for a security that enhance a security cultures of information (Alhogail et al. 2015). A sufficient security culture is necessary to lower a potential risk of harmful information interaction by employees, as they will develop knowledge, an understanding and a comprehension of precaution to advance their own skill levels correctly (Alhogail et al. 2015).

The information security culture forces researchers to utilise a variety of approaches that enhance a complete practice and a comprehension (Pevchikh, 2015). Accordingly, more research needs to provide a comprehensive view that guides and integrate all important factors that shape or have an impact on the effectiveness of the information security culture (Karlsson, 2014; Walton, 2015, (p.13)). Therefore, the current study provides an understanding of the information security culture and its elements that could reinforce an information security culture through developing a conceptual framework that could be used by researchers and practitioners as a starting point to understand how to cultivate and measure the information security culture. Initially, the paper provides background and related works in the literature that were published to identify various issues of the information security culture. Subsequently, it presents an initial proposal of a conceptual framework based on a comprehensive review. Finally, a conclusion and future works are discussed.

2. Literature Review and Theoretical Background

A comprehensive review has been conducted to identify the key literature relating to the information security culture, the exciting gaps in this area and to gain an understanding of frameworks and factors that are proposed in this field.

2.1. Culture of information security and the organisational culture

The concept of culture relates to the collective understanding that distinguishes individuals from different countries in accordance with anthropological social theories (Hofstede, 2001). It is possible to comprehend an organisational culture that defines employees' perceptions of their organisation, which develops with time through the influence of management and the individuals themselves (Schein, 2009). The culture is presented as a factor affecting the performance of individuals, adoption of information technology, integration process of information systems, information security management, knowledge transfers and change management (Hofstede, 2001). Moreover, a corporate or organisational culture helps to guide different employees' behaviour (Schein, 1999), as well as to influence what is determined to be acceptable in organisations. Various research studies analysed the

correlation that exist between the organisational and the information security culture and concluded that the organisational culture impacts greatly upon both the management of information security and its performance (Ruighaver et al. 2007).

2.2. Introduction to the information security culture

Most available studies show that the information security culture has been one of the most important approaches that can be used as guidance on how to protect assets, exerts an influence on the employee's behaviour with regard to a security and they concluded the need to consider it in organisations to manage a security in an effective way (Alhogail et al. 2015). Therefore, many researchers attempted to define the concept of an information security culture in different ways by using different theories and principles (Dhillon et al. 2016). Some researchers used Schein's model of organisational culture in defining the information security culture, such as Schlienger and Teufel (2003). They showed that an information security culture is a subset of organisation culture, concerned with three areas: artefacts and creations; collective values and knowledge; and basic assumptions and beliefs. Martins and Eloff's (2002) study noted that an information security culture is derived from the presumptions regarding perceived acceptable behaviour and characteristics which have an effect on how people deal with information security in organisations. Studies by Da Veiga and Eloff (2010), as well as Alhogail and Mirza (2014b) concluded that an information security culture is associated with employees' assumptions, attitudes, beliefs, values and knowledge that are used as guidance for undertaking activities to preserve information assets and impacting the behaviour of employees in an acceptable way by considering information security as a natural part of employees' daily activities.

Therefore, it is possible to infer that the concept of information security culture is related to artefacts, perceptions, attitudes, values, assumptions and knowledge that are held by employees in undertaking daily activities toward information security. However, it is important to clearly define what is meant by the two terms "security" and "culture" (Alnatheer et al. 2012). Schlienger and Teufel (2003) argued that measuring security and culture is a complex task, as generalisations are difficult to precisely define or measure the "culture". Thus, it is necessary to quantify and analyse the important factors which shape and measure an information security culture.

2.3. An overview of existing information security culture approaches

Implementing an effective culture is an essential step to create an adequate level of information security, as it affects the security practices and human behaviour. Many researchers have conducted different studies in the information security culture area, while literature reviews offer an overview of research that focuses on the information security culture, such as Alhogail and Mirza (2014b), Karlsson (2014) and Pevchikh (2015). Their literature analysis concluded that most investigated issues in information security culture relate to: the conceptualisation of the information security culture to identify the concepts and factors that affect or are affected by

information security culture, or to a cultivation of information security culture to assist organisations, observe the behaviour of people and examine the current culture, or an assessment of the information security culture to measure whether it is an adequate level to provide quality protection to the information assets.

There is a large volume of published studies that present different approaches and models that guide the researchers and the implementation of the information security culture. Some researchers focus only on developing an understanding of the concepts of information security culture (OECD, 2005; Tessem and Skaraas, 2005); on defining the information security culture (Kuusisto and Illoven, 2003); or providing a set of principles (Kraemer and Carayon, 2005; Ruighaver et al. 2007). Other researchers performed a study to illustrate a way in which to cultivate information security culture by developing a framework (Dojkovski et al. 2006; Da Veiga and Eloff, 2010; Alnatheer et al. 2012; Alhogail et al. 2015; Sherif et al. 2015) or to assess information security culture (Martins and Eloff, 2002; Schlienger and Teufel, 2005; Da Veiga and Eloff, 2010).

Most researchers used other theories as a basis to establish principles from other research areas by applying theories from different perspectives. One of the common theories is that an information security culture can be best represented by adopting Schein's model (Karlsson, 2014). The published studies generated various models and approaches that highlight information security culture's importance, promoted its benefits and provided guidelines for creating and assessing information security culture. However, the importance of creating information security culture resulted from a fact that a human dimension in an information security is always considered to be the weakest link (Da Veiga and Eloff, 2010). Many researchers concluded that it is important to understand how employees should behave and understand factors behind their behaviours to support the security of information assets (Alnatheer et al. 2012). The literature analysis showed that most available studies demonstrated that there are various important factors that could shape or change the information security culture (Alhogail and Mirza, 2014b).

As a result, it is essential to gain an overview of the current information security culture models and structures by conducting a comprehensive review that initiated the current study. The first aim is to investigate the conceptualisation of the information security culture. The second aim is to list and analyse the constructs that were provided in each study in the area of information security culture. The review of this study focuses on studies that assess information security culture to assist in developing a reliable and a valid framework. Thirteen studies were reviewed that presented essential knowledge in terms of identifying factors that assist in establishing the information security culture. These studies have been evaluated via important criteria: the development of an assessment instrument, a content validity, construct validity and reliability to identify an existing gap in the area and what constitutes a valid and a reliable framework. Table 1 summaries the list of research constructs for each study.

Research	Constructs/Findings
Martin & Eloff (2002)	Policy, benchmark, risk analysis, budget, management, trust, awareness, ethical conduct, change.
Chia et al. (2002)	Security budget, security expenditure, employee security awareness, security risk of staff, implementing security policy, making security suggestions, security ownership, audits.
Helokunnas & Kuusisto (2003); Kuusisto & Ilvonen (2003)	Security culture framework (Standardisation, Certification, Measurement of information security). Content components (People's attitude, Motivation, Knowledge, Communication, Compliance).
Schlienger & Teufel(2003, 2005)	Security culture has three layers: Corporate policies (policy, organisation structure, resources); Management (implementation of security policy, responsibility, qualification and training, awards and prosecutions, audits, benchmarks); Individual (attitude, communication, compliance).
OECD (2005)	Awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and reassessment.
Tessem & Skaraas (2005)	Long term plan, change management, top management, participation, branding, organisation culture.
Ruighaver et al. (2007)	Security governance framework (structural mechanism, functional mechanisms, social participation) Influences on security culture framework dimension (control, coordination, ownership, responsibility).
Dojkovski et al. (2006)	Individual and organisational e-learning; Ethical; national and organisational culture; Managerial (Policies and procedures, benchmarking, risk analysis, budget, management, response, training, education, awareness, change management); Behavioral (Responsibility, integrity, trust, ethnicity, values, motivation, orientation personal growth).
Kraemer &Carayon (2007)	Employee participation, training, hiring practices, reward system, management commitment, communication and feedback.
Da Veiga & Eloff (2010)	Leadership and governance (sponsorship, strategy, IT governance, risk assessment, ROI/metrics/measurement); security management and organisation (legal and regulatory, program organisation); Policy (policies, standard, procedure, guidelines, best practice, certification); security program management (monitor, audit, compliance); user security management (awareness, training, trust, privacy, ethical conduct); technology protection and operations (system development, technical operation, physical and environment, asset management, incident management, business continuity); change.
Alnatheer et al. (2012)	Factors influence ISC (Top management, policy enforcement, IS education and training); Factors reflect ISC (Security awareness, security ownership).
AlHogail et al.(2015)	Organisation dimension: management (policy, practice, communication); environment (national culture, standards and regulations, organisational culture); Employee dimension: preparedness (awareness and training, change); responsibility (reward, monitoring and control, acceptance).
Sherif et al. (2015)	National culture; organisational culture; Security compliance (IS behaviour, management support, policy, awareness and education, acceptance).

Table 1: Summary of proposed constructs in an information security culture

Most of these studies provide a comprehensive model and contribute a good understanding of how to create and assess an acceptable level of information security culture. Thirteen research perspectives relate to the creation of information security culture and five of them incorporate an assessment of information security culture. Most of these studies that are discussed focus on providing principles (Helokunnas and Kuusisto, 2003; Kraemer and Carayon, 2005; Kuusisto and Ilvonen, 2003; Tessem and Skaraas, 2005; OECD, 2005) that can be followed or develop frameworks (Alhogail et al. 2015; Alnatheer et al. 2012; Chia et al. 2002; Da Veiga and Eloff, 2010; Dojkovski et al. 2006; Ruighaver et al. 2007; Martins and Eloff, 2002; Sherif et al. 2015; Schlienger and Teufel, 2003), and are involved in identifying various factors that should be considered in order to establish or assess information security culture. They concluded that a particular information security culture is a product of various factors, such as top management, security policy, and security training that determine the individual's behaviour inside an organisation.

2.4. Limitation of current studies considering the information security culture factors

Most of the current studies develop a framework and demonstrate the importance of understanding factors that affect information security culture. However, there is no mutual agreement on factors that have to be considered for creating or assessing an information security culture. Only Alnatheer's study specifies factors that constitute information security culture. Minimal studies have used the same framework to create and assess information security culture. Studies by Alnatheer et al. (2012), as well as Da Veiga and Eloff (2010) provide an approach that uses the same framework to create and assess information security culture. Moreover, the two studies provide a statistically sound assessment instrument based on the defined framework to perform a security culture assessment. Also, Alnatheer's study is the only study perspective that validates his conceptual model using different validation techniques, such as a structural equation modelling in the information security culture field.

Furthermore, there is still limited coverage of other influencing factors. Factors have not been deeply considered in previous studies, such as individual difference variables and job satisfaction. The positive impacts of these factors and their contribution to a variety of workplace behaviours have been proved by several studies, such as D'Arcy and Greene (2009) and McCormac et al. (2017) studies. Also, McCormac et al. (2017) indicated that there is a need for future research that examines the potential interplay between the information security culture and the individual difference factors. Consequently, this study will cover other factors that can possibly influence information security culture. Based on the previous discussion, there is a need for more investigation in the area to provide comprehensive frameworks and best practices of an establishment and assessment of an information security culture, as there are calls in the literature to extend these areas of research.

3. A proposed information security culture framework

The aim of this study is to present a comprehensive reliable and valid framework that incorporates human behaviour and guides organisations in cultivating and assessing their information security culture. Therefore, this study proposed a comprehensive framework that considers the most important key human factors associated with information security culture suggested by the previous frameworks and adds new factors to see a potential link between these factors and an information security culture. The proposed framework in this study facilitates an understanding of information security culture and of elements that can reinforce information security culture. It provides management with a means to implement effective information security management approaches, which include the provision of guides and the implementation controls in understanding the importance of factors involved in the creation and measurement of the information security culture. By understanding the influential factors or the reflection factors, it is possible to aid in directing the interaction of humans with an information security. It will initially help to determine whether the level of the information security culture enhances the security of information assets, and will also assist in assessing the relationship between factors that influence the information security culture and factors that constitute the information security culture.

The development of a proposed framework was based on Alnatheer's model and on a comprehensive review of academic literature in regards to the area of information security culture. The reason for choosing Alnatheer et al.'s (2012) model is because it is the only study to specify what factors constitute an information security culture. Their research model was statistically tested for validity and reliability by using advanced techniques. Also, other studies have been developed by using Alnatheer's model, such as Walton's (2015) study. In the proposed framework, the information security culture comprises of several factors, as shown in Figure 1. The components of the framework are structured in three component categories comprising of the top-eight constructs/factors that are identified and have a positive impact on the creation of the information security culture from thirteen studies, where there is a strong agreement among the academic researchers. For each study, all the identified constructs were extracted and counted in Table 2 to identify the top critical success factors as potential candidates in the conceptualisation of an information security culture. Five constructs (top management, security policy, education and training, security awareness and security ownership) have been adopted from Alnatheer's model. These five constructs have been proven to have a positive impact on the information security culture (Martin and Da Veiga, 2015). The other identified constructs, such as a risk assessment, ethical conduct and security ownership, have not proven its impact on information security culture, although it has been signified as important to consider it when cultivating or measuring the information security culture.

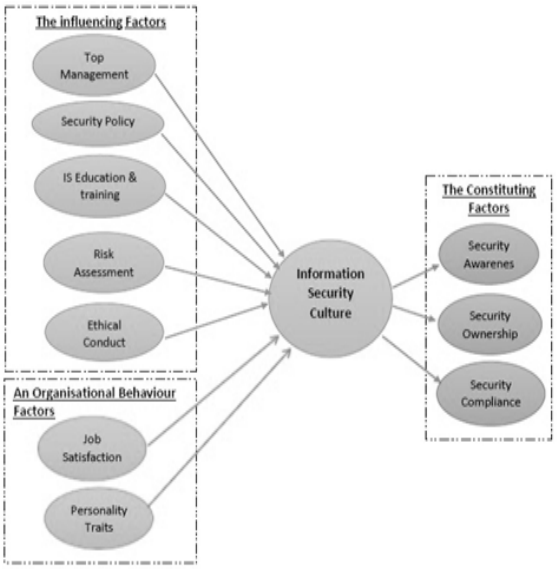

Figure 1: The comprehensive information security culture framework

In addition, there are other factors that contribute to a variety of workplace behaviours, such as personality traits and job satisfaction. Based on the previous studies, such as Alnatheer et al. (2012) and Martin and Da Veiga (2015), it was concluded that there is a strong correlation between information security culture and security awareness. Meanwhile, the study of McCormac et al. (2017) revealed the impact of personality on information security awareness. Additionally, the study of D'Arcy and Greene (2009) revealed that there is a strong correlation between information security culture, security compliance and the behavioural role of employees, which also stated that the higher job satisfaction can motivate employees' behaviour to comply with security requirements. Yet, these two factors have received little attention from scholars in the area of information security culture. Hence, this study predicts that the personality traits and job satisfaction may positively influence the information security culture. In order to see how a potential interplay between these two factors and an information security culture exists, these two factors have been added as candidate constructs to the framework. The rationale for grouping the components is further based on a model proposed by Alnatheer et al. (2012), as well as D'Arcy and Greene (2009).

Constructs	Number of Times Cited out of 13 studies	Construct Ranking
Top Management	8	1
Security Policy	8	1
Security Education & Training	8	1
Security Awareness	8	1
Security Ownership	7	5
Security Risk Analysis & Assessment	6	6
Ethical Conduct	5	7
Security Compliance	5	7

Table 2: Top candidate constructs in the information security culture research

The total identified constructs/factors are:

* Top Management refers to a degree of how the senior leadership understands the importance of the information security function and is involved in the security activities to improve and create a strong information security culture (Martin and Da Veiga, 2015).

* Security Policy is a written document that has to be central to its foundation, which specifies the organisation's strategies and requirements of the security approach that guide both the management and employees' behaviour (Da Veiga, 2015).

* Security Education and training is a learning process that provides general knowledge of a certain subject related to the security environment and the required security skills for employees to perform the security procedures (Da Veiga and Martins, 2017).

* Risk Analysis and assessment defined as when countermeasures are adequate to decrease the probability of loss; when it affects to an acceptable level and helps organisations and its employees to become capable of understanding potential damage to the security, which helps to create an awareness of the information security culture (Da Veiga and Eloff, 2010; Martins and Eloff, 2002).

* Ethical Conduct refers to the values and rules that help to distinguish the accepted right by an organisation (Alnatheer et al. 2012; Martins and Eloff, 2002).

* Personality Traits describe the personality factors, their potential factors and helps to understand the variability between individuals to understand the underlying psychological mechanisms which might affect user behaviour with regard to information security (McCormac et al. 2017).

* Job Satisfaction refers to the overall sentiment of 'well-being' in the workplace and helps to determine how an employee can adapt to situational factors, such as remaining committed, which can prove detrimental to organisations (D'Arcy and Greene, 2009).

* Security Awareness defined as when users understand the potential of information security-related issues and become aware of their security mission that leads to the commitment to the ideal (Da Veiga and Martins, 2017).

* Security Ownership refers to how employees view their responsibilities, their roles in security and their willingness to act in a supportive manner to enhance their own security performance and the organisation's performance (Alnatheer et al. 2012).

* Security Compliance refers to how the employees' behaviour complies with the security policy, regulations and security practices in order to reduce the security breaches that are caused by employees' misbehaviour, as well as to improve information security culture inside organisations (Furnell and Thomson, 2009; Da Veiga and Martins, 2017).

These constructs appear to be the most influential factors and are considered as part of the information security culture's conceptualisation. In a study framework, there is a clear distinction between factors that constitute and factors that influence information security culture, together with new factors that relate to an organisation's behaviour category that may influence the information security culture. However, there is strong evidence that the identified factors were derived from the literature review analyses that have a positive influence upon the information security culture. For instance, several researchers indicate the importance of top management commitment to cultivate an information security culture (D'Arcy and Greene, 2009). Others revealed the strong influence of policy on an information security culture creation (Da Veiga, 2015). Moreover, the security education and training can influence the information security culture cultivation (Da Veiga and Martins, 2017). Finally, Martins and Eloff (2002) found that the ethical conduct policies were important factors that influence information security culture. These factors have a positive influence on each other, and in turn have a positive influence on the information security culture. Simultaneously, the formed information security culture will have its influence on certain factors. Ultimately, the relationships between factors will be tested statistically to determine whether a proposed framework is valid.

4. Conclusion and future work

The review of the information security culture research illustrates that more efforts are needed for additional investigation in the area, especially as most of the existing frameworks are fragmented and usually take a limited view of the involved issues. Most existing studies develop a comprehensive model and contribute a good understanding of how it is possible to create and maintain an acceptable level of an information security culture. The literature review revealed that there are a limited number of studies that develop a framework that can be used for both the creation and assessment of information security culture to ensure the effectiveness of an approach and content validity. Moreover, there is no mutual agreement on factors that have to be considered in the creation or measurement of an information security culture. Therefore, the current study proposes a framework that integrates the most important factors and distinguishes between factors that constitute and factors that influence information security culture. In the future, it is planned to extend and examine the proposed framework by applying an interview to develop a framework and assist in the identification of other factors that might emerge after analysing a qualitative interview.

5. References

Alhogail, A., Mirza, A. and Bakry, S.H. (2015), *"*A comprehensive human factor framework for Information Security in organisations", *Journal of Theoretical and Applied Information Technology*, Vol. 78, No. 2, pp201.

Alhogail, A. and Mirza, A. (2014b), "Information security culture: A definition and a literature review*", Computer Applications and Information Systems,* pp. 1-7.

Alnatheer, M., Chan, T. and Nelson, K. (2012), "Understanding And Measuring Information Security Culture*"*, *Pacific Asia Conference on Information Systems,* pp144.

Chia, P.A., Maynard, S.B. and Ruighaver, A.B. (2002), "Understanding organisational security culture", Sixth *Pacific Asia Conference on Information Systems,* pp731-740.

Connolly, L., Lang, M., Gathegi, J. and Tygar, D.J. (2017), "Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study*", Information and Computer Security,* Vol.25, No. 2, pp118-136.

D'Arcy, J. and Greene, G. (2009), "The multifaceted nature of security culture and its influence on end user behaviour", *IFIP TC8 International Workshop on Information Systems Security Research,* pp145-157.

Da Veiga, A. (2015), "The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study", *Proceedings of the Ninth International Symposium on Human Aspects of Information Security and Assurance,* pp.22–33.

Da Veiga, A. and Eloff, J.H. (2010), "A framework and assessment instrument for information security culture", *Computers & Security*, Vol. 29, No. 2, pp196-207.

Da Veiga, A. and Martins, N. (2017), "Defining and identifying dominant information security cultures and subcultures ", *Computers & security*, Vol.70, pp72-94.

Dhillon, G., Syed, R. and Pedron, C. (2016), "Interpreting information security culture: An organizational transformation case study", *Computers and security*, Vol.56, pp63-69.

Dojkovski, S., Lichtenstein, S. and Warren, M. (2006), "Challenges in fostering an information security culture in Australian small and medium sized enterprises", *5th European conference on Information Warfare and Security,* pp31-40.

Furnell, S. and Thomson, K.L. (2009), "From culture to disobedience: Recognising the varying user acceptance of IT security*"*, *Computer Fraud and Security*, Vol.2009,No.2,pp5-10.

Helokunnas, T. and Kuusisto, R. (2003), "Information security culture in a value net", *Engineering Management Conference*, pp190-194.

Hofstede, G. (2001), "Culture's recent consequences: Using dimension scores in theory and research*", International Journal of cross cultural management*, Vol. 1, No. 1, pp11-17.

Information Security Breaches Survey. (2015), "Information Security Breaches Survey", www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html, (Accessed 01 February 2016)

Karlsson, F. and Hedström, K. (2014),*"*End user development and information security culture*", International Conference on Human Aspects of Information Security, Privacy, and Trust,* pp246-257.

Kraemer, S. and Carayon, P. (2005), "Computer and information security culture: findings from two studies*", the Human Factors and Ergonomics Society Annual Meeting,* Vol. 49, No. 16, pp1483-1488.

Kuusisto, T. and Ilvonen, I. (2003), "Information security culture in small and medium size enterprises*", Frontiers of E-business Research*.

Martins, N. and Da Veiga, A. (2015), "An Information Security Culture Model Validated with Structural Equation Modelling", *Proceedings of the Ninth International Symposium on Human Aspects of Information Security and Assurance,* pp.11–21.

Martins, A. and Eloff, J. (2002), "Assessing Information Security Culture*", Information for Security for South-Africa 2nd Annual Conference,* pp1–14.

McCormac, A., Zwaans, T., Parsons, K., Calic, D. and Butavicius, M. (2017), "Individual Differences and Information Security Awareness", *Computers in Human Behavior*, Vol. 69, pp151-156.

OECD. (2005), "The promotion of a culture of security for information systems and networks in OECD countries*",* www.oecd.org/internet/ieconomy/35884541.pdf, (Accessed 15 June 2016)

Parsons, K., Calic, D., Pattinson, M., Pattinson, M.., Butavicius, M., McCormac, A. and Zwaans, T. (2017.), "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies)", *Computers and security*, Vol.66, pp40-51.

Pevchikh, E. (2015), "Information Security Culture: Definition, Frameworks and Assessment: A Systematic Literature Review", Master thesis, Luleå University of Technology.

Ruighaver, A.B., Maynard, S.B. and Chang, S. (2007), "Organisational security culture: Extending the end-user perspective*", Computers and Security*, Vol. 26, No.1, pp56-62.

Schein, E.H. (2009), *The corporate culture survival guide*, Jossey-Bass, San Francisco, U.S.A., ISBN: 9780-470-29371-3.

Schlienger, T. and Teufel, S. (2003), "Information security culture-from analysis to change", *South African Computer Journal*, Vol. 31, pp46-52.

Schlienger, T. and Teufel, S. (2005), "Tool supported management of information security culture", *Security and Privacy in the Age of Ubiquitous Computing*, pp65-77.

Sherif, E., Furnell, S. and Clarke, N. (2015), "An identification of variables influencing the establishment of information security culture*", International Conference on Human Aspects of Information Security, Privacy, and Trust,* pp436-448.

Tessem, H.M. and Skaaraas, K.R. (2005), "Creating a security culture*", Information Society and Security*, p15.

Walton, H. (2015), *Security Culture: A How-to Guide for Improving Security Culture and Dealing with People Risk in Your Organisation*, Gower Publishing Limited, Surrey, U.K., ISBN: 978-1-4094-6562-1.