A Systematic Literature Review: Information Security Culture

Amjad Mahfuth
College of Computer Science and Information Technology
Universiti Tenaga Nasional,
Putrajaya, Malaysia
Amahfouth99@gmail.com

Salman Yussof, Asmidar Abu Baker and Nor'ashikin Ali
College of Computer Science and Information Technology
Universiti Tenaga Nasional,
Putrajaya, Malaysia
Salman@uniten.edu.my, Asmidar@uniten.edu.my and Shikin@uniten.edu.my

***Abstract*—Human behavior inside organizations is considered the main threat to organizations. Moreover, in information security the human element consider the most of weakest link in general. Therefore it is crucial to create an information security culture to protect the organization's assets from inside and to influence employees' security behavior. This paper focuses on identifying the definitions and frameworks for establishing and maintaining information security culture inside organizations. It presents work have been done to conduct a systematic literature review of papers published on information security culture from 2003 to 2016. The review identified 68 papers that focus on this area, 18 of which propose an information security culture framework. An analysis of these papers indicate there is a positive relationship between levels of knowledge and how employees behave. The level of knowledge significantly affects information security behavior and should be considered as a critical factor in the effectiveness of information security culture and in any further work that is carried out on information security culture. Therefore, there is a need for more studies to identity the security knowledge that needs to be incorporated into organizations and to find instances of best practice for building an information security culture within organizations.**

Keywords — Attitudes, Security knowledge, Information Security culture, Human Behavior.

I. INTRODUCTION

Nowadays, Information is considered to be very essential for organizations to the extent that it's regarded as a key asset of a given organization [1]. Therefore protecting this information is crucial to ensure the stability of the organization and to maintain the availability, integrity and confidentiality of that information. A recent study by Ponemon Institute (2015) indicates that many organizations have lost billions of dollars as a result of information breaches or information violations. These breaches have also had some negative effects on customer trust. Among the major threats that face an organization are the employees' perceptions, behaviors and performance especially when they interact with the organization's assets. A study on data breach investigation reports indicates that employees inside organizations could be responsible for most of the data breaches that occur, whether intentionally or unintentionally [3]. Moreover, many studies [4]–[7] have concluded that insiders can pose many threats to the safety of information inside an organization.

In information security the human element consider the most of weakest link in general [4], [8], [9]. Hence concentrating only on technical measures to protect an organization's assets without any consideration of the human factor is clearly inadequate. Human error and human negligence are the cause of different types of data breach inside organizations [10], [11]. Thus, on one hand employees play a prominent role to in creating threats to an organization and on the other hand can play a key part in protecting against or preventing such breaches. Therefore, organizations should focus on employees' behavior, attitudes, assumptions and awareness in order to establish an information security culture. Essentially, the effectiveness of any type of security system depends on employee behavior towards organization's information assets [12].

Creating an information security culture within an organization will minimize the harmful interaction of employees towards organization's information assets. Further, it will reduce the risk of employee misbehavior when they interact with the organization's assets (Van Niekerk & Von Solms, 2010; Verizon, 2014). Numerous studies indicate that the user's attitude and lack of security awareness are the most significant contributors to security incidents [13]. Such findings support the need to instill an information security culture in order to influence employees' security behavior within organizations.

Some studies [14], [15] argue that security of information can be protected and managed if an effective information security culture is taken into consideration and the employees are able to recognize, know, understand and manage their own perceptions so as to secure their organization's assets. The key to establishing such a culture lies in giving employees the required security knowledge and the specified skills they need for interacting with the organization's assets. Doing so will help to influence the employees' security behavior and protect the organization's assets. Therefore, numerous studies need to be conducted in this area in order to find ways to create an efficient information security culture within organizations. Moreover, the organizations themselves should develop some

978-1-5090-6255-3/17/$31.00 ©2017 IEEE

visions and strategies for the adoption and implementation of an information security culture by their employees. A lot of studies [4], [16]–[18] have focused on the significance of implementing an effective information security culture within organizations to minimize the security risks posed to organizational information assets.

This paper adopted the systematic literature review (SLR) approach to investigate and understand the approaches, definitions, factors and frameworks for formulating and building an information security culture within organizations in order to find the knowledge gap. In addition, the SLR identified different methodologies and empirical studies that aimed at exploring the nature of information security culture. The SLR in particular focused on issues related to information security culture in papers and studies that were published between 2003 - 2016.

The remainder of the paper is organized as follows: In section 2, the research method adopted to conduct the SLR is described. Then in section 3 the definitions of information security culture are presented, followed by an overview of the frameworks that have been proposed thus far in section 4. This is followed by a discussion of the current thinking and way forward on establishing an information security culture in organizations in section 5. Finally, in section 6, the conclusion is inclusive of both summary and future work.

II. Research method

For the present study, the relevant literature on information security culture was collected so as to be reviewed and analyzed systematically through using the so-called qualitative content analysis. This type of analysis utilizes a subjective interpretation of the text content by means of using a systematic classification process of coding to identify certain themes or patterns in that text.

In order to carry out the search process the researcher focused on the content of electronic databases such as Springer, Google Scholar, ACM and IEEE Electronic Library. The SLR was applied to papers published from 2003 to 2016 by using keywords related to information security culture. A qualitative content analysis was used to identify and classify the papers accordingly.

Our search initially identified 68 papers that focus on information security culture. However, because the goal of conducting the SLR was to investigate the frameworks, methodologies and factors that affect information security, we filtered these papers further. As a result, it was found that 18 papers (27% of the papers) mainly concentrated on the framework of information security culture. The other papers focused on other topics, such as definitions of information security culture, key factors influencing information security culture, challenges of information security culture, the relationship between organizational culture and information security culture, the cultivation process for implementing information security, general issues regarding information security culture, and assessment instruments for information security culture. Some of the papers also conducted empirical studies on information security culture includes data collection and analysis. Before discussing the information security culture frameworks that have been proposed, it would be useful first to present the various definitions of information security culture that exist in the literature.

III. Information security culture definitions

Information security culture is one of the most prominent issues in organizational culture. Information security culture is classified as a subculture of an organization and it includes the daily tasks, activities, guidelines and practices of the employees in an organization which should help them to protect the organization's information assets and reduce the risks to those assets [18].

Since the concept of information security culture is somehow still new [19], information security culture is often explained by using a collection of different theories and disciplines drawn from other research areas. Some researchers such as [14], [20]–[22] argued the information security culture should be achieved as a goal to create an embedded culture that includes all the activities and guidelines needed for information security to become one of the natural daily activities and duties of each employee in an organization. In other studies [9], [19] information security culture is described as tasks and activities that should be done in parallel by employees and the organization as whole with the aim of achieving consistency and compatibility with information security principles.

In another definition, [23] describes information security as "The collection of human attributes such as behaviors, attitudes, and values that facilitate the protection of all the information in the organization". [24] define information security culture more fully as "The attitudes, assumptions, beliefs, values and knowledge that employees use to interact with the organization's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior evident in the artifacts and creations that become part of the way things are done in the organization to protect its information assets".

[25] suggest that information security culture is "The way our minds are programmed that will create different patterns of thinking, feelings and actions for providing the security process", while[15] define information security culture as "The collection of perceptions, attitudes, values, assumptions and knowledge that guide how things are done in the organization in order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees' security behavior in a way that preserving the information security becomes a second nature".

Another definition is provided by [9], who see information security culture as "The perceptions, attitudes and assumptions that are accepted, adopted and encouraged by the employees in the organizations in relation to the information system".

Malcomson [26] argues that the "Security culture is candidate by the assumptions, values, attitudes and beliefs held by the employees of an organization and their behavior could potentially impact the security of that organization and that may or not may have an explicit known link to that impact".

978-1-5090-6255-3/17/$31.00 ©2017 IEEE

Based on the presented definitions of information security culture, we can view information security culture as an integration process of beliefs, perceptions, attitudes, values, assumptions and knowledge that guide, direct and manage employees' perceptions and attitudes to influence employees' security behavior or to find an acceptable behavior for employees when they are interacting with the information assets in their organizations. In other words, this culture should be instilled and practiced daily by the employees of an organization, whereby the organization and its employees must work closely together in order to establish a conducive environment for information security culture to be inculcated throughout the organization.

IV. Information security culture frameworks

The literature review identified 18 papers that concentrate on the information security culture framework. The frameworks presented in the papers are based on different assumption and issues. The following paragraphs summarize those frameworks.

Ruighaver et al. (2007) developed a framework based on the dimensions of the [27] organizational culture framework, namely, truth, time, motivation, stability, control and orientation, which it is argued improve one's understanding of an organization's security culture and the steps required to move toward such an organizational culture. Each of the identified dimensions was investigated with regard to its utility to construct information security culture. The authors argue that an ideal security culture in an organization should be achieved to make a balance between different factors of organizations.

[28] presented a framework based on Schein's (1992) model related to organizational culture theory that intended to explore how security governance affects security culture specifically in terms of responsibility and ownership of security. The authors found that the structural and functional mechanisms in security governance are the most influential factors.

[29] presented a framework that was designed to enhance the implementation of information security culture in small and mid-sized enterprises (SMEs) in Australia. They present details of the challenges of developing a security culture in SMEs. Moreover, the researchers identified other factors that have some impacts on information security culture, such as national and ethical culture, governmental initiatives in raising awareness and information security benchmarks, and vendors who may demonstrate a sense of trustworthiness to SMEs as external factors. Furthermore, they identify internal influencing factors that have high impacts on information security culture, which include governance and organizational culture. In addition, they provide management factors, such as a security policy and a budget. They also provide earning factors for individuals in an organization, such as e-learning, training, awareness and education for developing and fostering an effective background for the implementation of an information security culture in enterprises. Finally, they argue that it is necessary for top management to focus on fostering awareness among employees regarding information security culture and that top management should have strategic plans in place to ensure information security culture can be inculcated within organization.

Zakaria (2006) provided a framework based on Schein's (1992) model related to organizational culture where the aim of the framework is to develop the data collection methods for research studies on information security culture across organizations. The author recommends using the questionnaire, semi-structured interview, direct observation or document review methods.

Another framework presented by Chang and Lin (2007) seeks to test the relationship between organizational culture and information security management in order to indicate the impacts of organizational culture traits on the effective implementation of ISM. The authors concluded that the most organizational features should involve cooperation, innovation, consistency and effectiveness.

Chen, Ramamurthy and Wen (2015) proposed a research model to investigate the influence of information security awareness programs with respect to engendering a security culture. The result indicates that security education, training and awareness (SETA) programs as well as security monitoring have a positive impact on security culture and employees' awareness with respect to organizational security policy. Moreover, they found that there is a positive relationship between awareness of security monitoring and security culture. The aim of their framework is to help to establish an information security culture within organizations.

Chia, Maynard and Ruighaver (2002) proposed a framework using on [27]'s organizational culture framework which focused on raising information security awareness with in organization so as to examine the impact of organizational culture on information security culture. The authors conclude that administration support and employee awareness are the most critical factors for information security culture. However, they do not suggest any solutions as to how the quality of the information security culture within organizations could be enhanced. Schlienger and Teufel (2003) provided a framework based on internal marketing which aimed to analyze information security culture in an organization for the purpose of creating and enhancing that culture. Their framework based on Schein model contains many steps: the first step is pre-evaluation, the second is a strategic plan, the third is an operative plan, and the fourth and fifth are implementation and post-evaluation. These steps are subject to change, evaluation or maintenance. However, their study lacks a practical experiment to test the execution of the suggested framework and to examine whether it can be changed or maintained practically in an organizational security culture.

Alnatheer and Nelson (2009) provided a framework that aims to understand information security culture and its best practices in Saudi Arabia. The framework presented provides some important steps toward achieving ISM and details of the cultural factors that would facilitate the establishment of an information security culture within an organization. The main idea of the provided framework is to ensure a security culture has been included in the daily practices of organizations of Saudi Arabia. Moreover, they present some main factors, such as organization's governance, regulatory and legal

978-1-5090-6255-3/17/$31.00 ©2017 IEEE

environment, and other corporates. Finally, they concluded the national culture has impact on organization culture as well as it has impact to security culture.

[30] provided a framework that helps organizations to determine whether the required information security culture is incorporated within organization culture. They also investigated the relationship between the two cultures. Their framework is based on [27]'s eight-dimensional organizational culture framework. The authors argue the importance of instill the concept of information security culture across organizations that's aim to influence employees' security behavior and actions.

[4] presented a more comprehensive framework to evaluate and enhance an information security culture practically within organizations. First, they identified several information security components that organizations should adopt, such as process, human and technical threats that would disturb the establishment of an effective information security culture across an organization. Later, these components were classified into categories that cover each individual, each group and organizational ties of information security behavior within this organization. This framework describes the embedding of information security culture in the organization. However, the framework is lacking as it does not illustrate the internal relations and the expected influences of the different information security components.

[31] provided a comprehensive framework for creating effective security for health information systems based on security culture and security awareness. The aim of the framework is to enhance human behavior by providing a security awareness and security culture in the e-health information system. They suggest that security awareness and security culture are the most important aspects to focus on in order to establish an effective health information security framework. However, their proposed framework lacks depth with respect to identifying the components and the factors and the associated relations between them.

[1], [32], [33] investigated information security culture by providing an integrated model of Bloom learning taxonomy. Their framework, which is based on Schein's model. In addition, they argue that to provide an effective information security culture within organizations, it is necessary to provide information security knowledge to employees, which could be seen as a fourth layer of Schein's model, namely, the knowledge layer. The aim of their studies is to establish an effective information security culture within organizations. They discussed the Schein model describes the organizational culture instead of information security culture.

[34] suggested framework for identifying the specifications of organizational culture subject to information security practices by means of determining the knowledge, skills and activities of individuals that may influence and enhance individual and group practices in terms of the management of information security culture. This conceptual model concentrated on the impact of the national culture on the organizational culture. They identify four types of behavior: the " Knowing-Not doing, Not knowing-Doing, Not doing mode and finally Knowing-Doing mode". Furthermore, they argue that the behavior of employee's could change from one mode to another depending on the employee's role, technology available in the organization, and the situation and awareness regarding security training.

Another conceptual model was presented by [35] for ISM e-learning, which focuses on people's cultural views. Their model describes the relationships between the dimensions related to e-learning stakeholders in ISM. Furthermore, the presented model addresses people's behaviors and their real views. Finally, the authors identify the dimensions of conceptual model, such as threats, stakeholders, cultural view, and ISM elements.

[36] provided a framework that focuses on security behavior based on assumptions, attitudes, as well as the "human factor diamond" that includes management, responsibility, preparedness, society and regulations. The proposed integrated framework combines human, organization, strategy and technology factors in order to help organizations to implement and adopt an information security culture. The framework presented includes most of the issues related to human behavior that would help to establish a secure situation for information assets in organizations. These issues are covered in a systematic way by using the STOPE model, which refers to strategy, technology, organization, people and environment, to ensure that the framework is comprehensive. Later, these issues are translated into specific activities and tasks with respect to the human factor diamond. Furthermore, the principles of change management are provided in addition to the process of cultivation that guides the information security culture within the organization.

[37] also developed a human factor framework. In their work they focus on factors has effective impacts to end users' behavior, namely, lack of awareness, lack of motivation, belief, behavior and inadequate of technology In addition, the authors indicate that the most important issue for an organization to address is the fostering of security awareness among employees through education. Moreover, it was found that the weakest link in security area was the human factor which made them to suggest some factors that can influence human acts in organizations.

[38] presented a conceptual model specifically for the healthcare environment. Based on a literature review, they identify numerous factors that influence information security culture, namely, information security awareness, behavior, change management, knowledge, organizational system and security requirements. However, their framework appears to fail to identify the relationships between the factors and their impacts on information security culture.

From the above it is apparent that most of the 18 identified frameworks attempt to address numerous issues and many factors have a relation with information security culture. Moreover, different environments and different assumptions are considered to formulate each information security culture framework. For instance, some of the frameworks are highly focused on addressing human factors, such as providing awareness, training and education programs for employees, whereas some papers focus on the external factors that influence information security culture.

978-1-5090-6255-3/17/$31.00 ©2017 IEEE

V. Discussion

From our analysis of the literature, it is clear that the human factor is considered the weakest link in the security chain. Employees inside the organization is considered to be the main threat to organization's assets[4], [9]. Moreover, [11] argue that human error is the cause of numerous data breaches in organizations and that employees play a significant role in creating or preventing threats to an organization. The information security culture influences the employee's security behavior. Thus, human behavior within an organization is guided by the required knowledge. Therefore, knowledge is a very important factor in managing the perceptions, attitudes and behaviors that guide employees' interactions with organizational assets. Human behavior must be directed by knowledge in order to minimize the risks posed by the insider (the employee). In order to establish an acceptable and effective information security culture, it is necessary to focus on improving human security behavior in organizations through focusing on the required knowledge for the employees.

This is in line with the view of [1] who added a new fourth layer to Schein 's model, namely a knowledge layer, because the Schein model, which consists of three layers, describes organizational culture and not information security culture. The addition of a fourth layer enables the enhanced model to describe information security culture instead of organizational culture. Most of the frameworks identified by the SLR were developed based on Schein's three-layer model. Therefore, there is a lack of research on information security culture that considers knowledge as important factor, as suggested by [1].

More recently, [36] has focused on the relationship between knowledge and behavior in information security culture. The author concludes that there is a positive relationship between levels of knowledge and how employees behave. Therefore, the level of knowledge significantly affects information security behavior and culture and should be considered as a critical factor in the effectiveness of information security culture and in any further work that is carried out on information security culture. The work of [36] strongly supports the findings of [1]. It should be mentioned that [39] argue that every employee needs to understand the importance of establishment information security in order to protect the organization's assets. Thus, it is necessary to impart information security knowledge to employees. Other studies, [18] and [40], also mention that there is a relationship between knowledge and behavior but they do not provide any further details or undertake any investigation on the type of knowledge that should be inculcated to enhance employee behavior in respect to information security culture in organizations.

The above indicates that employees must have an appropriate behavior and attitude toward information security and that this can be acquired by providing security knowledge to employees. Knowledge and behavior should be in line so that organizations can have an effective information security culture. However, there is a lack of research on what security knowledge required should be imparted in order to influence human behavior and to focus on what the impacts of security knowledge are on human behavior in information security culture. Therefore, there is still a gap in security knowledge that needs to be discovered by further research.

Furthermore, most of the factors in the existing frameworks have been linked directly with the information security culture framework without any focus on knowledge and human behavior as important factors that can help to enhance information security culture. Referring to the definitions of information security culture, it is apparent that human behavior has the ability to accept/do or reject/fail to do a task in information security in the organization. Therefore, human behavior is affected by knowledge. Since there is a correlation between human behavior and knowledge, it is more crucial to focus on the security knowledge required within organizations to inculcate an information security culture.

VI. Conclusion

The objective of this paper was to conduct SLR of the works on information security culture published between 2003 –2016. The review revealed the necessity to construct an information security culture within organizations in order to protect them from the inside and to influence employees' security behavior. It was also revealed that effective information security culture has the potential to enhance employees acting in effect as a 'human firewall' that can help to protect organizational information assets. Establishing an information security culture should involve changing the existing culture so that it is more effective in respect of addressing security issues. This may require a change in the behavior and attitude of employees when they are interacting information assets. Therefore, there is a need for more studies to identity the security knowledge that needs to be incorporated into organizations and to find instances of best practice for the establishment of an information security culture within organizations. It is hoped that the review provided in this paper will assist researchers who are interested in investigating this field further.

References

[1] J. F. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," Comput. Secur., vol. 29, no. 4, pp. 476–486, 2010.

[2] Ponemon Institute, "2015 Cost of Data BreachSstudy: Global Analysis," no. May, pp. 1–30, 2015.

[3] Verizon, "2014 Data Breach Investigations Report," Verizon Bus. J., vol. 2014, no. 1, pp. 1–60, 2014.

[4] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," Comput. Secur., vol. 29, no. 2, pp. 196–207, 2009.

[5] G. Božić, "The role of a stress model in the development of information security culture," in MIPRO, 2012 Proceedings of the 35th International Convention, 2012, pp. 1555–1559.

[6] S. Furnell, "End-user security culture: a lesson that will never be learnt?," Comput. Fraud Secur., vol. 2008, no. 4, pp. 6–9, 2008.

[7] A. Da Veiga, N. Martins, and J. H. P. Eloff, "Information security culture – validation of an assessment instrument," South African Bus. Rev., vol. 11, no. 1, pp. 147–166, 2007.

[8] B. Schneier, "Secrets and Lies: digital security in a networked world. 2000," New York, John Wiley Sons. Rocco F. Grillo, CISSP Manag. Dir., vol. 2, no. 2.603, p. 838.

[9] A. Martins and J. Elofe, "Information security culture," in Security in the information society, Springer, 2002, pp. 203–214.

978-1-5090-6255-3/17/$31.00 ©2017 IEEE

[10] G. N. Samy, R. Ahmad, and Z. Ismail, “Threats to health information security,” in Information Assurance and Security, 2009. IAS’09. Fifth International Conference on, 2009, vol. 2, pp. 540–543.

[11] A. Appari and M. E. Johnson, “Information security and privacy in healthcare: current state of research,” Int. J. Internet Enterp. Manag., vol. 6, no. 4, pp. 279–314, 2010.

[12] M. Boujettif and Y. Wang, “Constructivist approach to information security awareness in the Middle East,” in Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on, 2010, pp. 192–199.

[13] B. Kitchenham and S. Charters, “Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3,” in Engineering, vol. 45, no. 4ve, 2007, p. 1051.

[14] B. Von Solms, “Information security--the fourth wave,” Comput. Secur., vol. 25, no. 3, pp. 165–168, 2006.

[15] A. Alhogail and A. Mirza, “Information Security Culture: A Definition and a Literature review,” Comput. Appl. Inf. Syst., no. January, pp. 1–7, 2014.

[16] A. B. Ruighaver, S. B. Maynard, and S. Chang, “Organisational security culture: Extending the end-user perspective,” Comput. Secur., vol. 26, no. 1, pp. 56–62, 2007.

[17] I. Okere, J. Van Niekerk, and M. Carroll, “Assessing information security culture: A critical analysis of current approaches,” in 2012 Information Security for South Africa, 2012, pp. 1–8.

[18] O. Zakaria, “Internalisation of information security culture amongst employees through basic security knowledge,” IFIP Int. Fed. Inf. Process., vol. 201, pp. 437–441, 2006.

[19] L. Ngo, W. Zhou, and M. Warren, “Understanding Transition towards Information Security Culture Change.,” in Proceeding of the 3rd Australian Computer, Network & Information Forensics Conference, Edith Cowan University, School of Computer and Information Science, 2005, pp. 67–73.

[20] C. Vroom and R. Von Solms, “Towards information security behavioural compliance,” Comput. Secur., vol. 23, no. 3, pp. 191–198, 2004.

[21] T. Schlienger and S. Teufel, “Information security culture-from analysis to change,” South African Comput. J., no. 31, p. p--46, 2003.

[22] K.-L. Thomson, R. Solms, and L. Louw, “Cultivating an organizational information security culture,” Comput. Fraud Secur., vol. 2006, no. 10, pp. 7–11, 2006.

[23] G. Dhillon, Principles of Information Systems Security: text and cases. Wiley New York, NY, 2007.

[24] A. Da Veiga and J. H. P. Eloff, “A framework and assessment instrument for information security culture,” Comput. Secur., vol. 29, no. 2, pp. 196–207, 2010.

[25] B. Al Sabbagh, M. Ameen, T. Wätterstam, and S. Kowalski, “A Prototype For HI 2 Ping Information Security Culture and Awareness Training,” in e-Learning and e-Technologies in Education (ICEEE), 2012 International Conference on, 2012, pp. 32–36.

[26] J. Malcolmson, “What is security culture? Does it differ in content from general organisational culture?,” in 43rd Annual 2009 International Carnahan Conference on Security Technology, 2009, pp. 361–366.

[27] J. R. Detert, J. G. Schroeder, and J. J. Mauriel, “A framework for linking culture and change initiatives in organizations,” Acad. Manag. Rev., vol. 25, no. 4, pp. 850–863, 2000.

[28] K. Koh, a. Ruighaver, S. Maynard, and a. Ahmad, “Security Governance : Its Impact on Security Culture,” in Proceedings of The third Australian Information Security Management Conference, 2005, pp. 1–12.

[29] S. Dojkovski, S. Lichtenstein, and M. J. Warren, “Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia.,” in ECIS, 2007, pp. 1560–1571.

[30] J. Lim, S. Chang, S. Maynard, and A. Ahmad, “Exploring the relationship between organizational culture and information security culture,” in Proceedings of the 7th Australian Information Security Management Conference, 2009, no. December, pp. 88–97.

[31] A. B. Shahri, Z. Ismail, and N. Z. A. Rahim, “Security culture and security awareness as the basic factors for security effectiveness in health information systems,” J. Teknol. (Sciences Eng., vol. 64, no. 2, pp. 7–12, 2013.

[32] J. Van Niekerk and R. Von Solms, “Understanding Information Security Culture,” Proc. ISSA 2006 from Insight to Foresight Conf., 2006.

[33] J. Van Niekerk and R. Von Solms, “A holistic framework for the fostering of an information security sub-culture in organizations,” Issa, pp. 1–13, 2005.

[34] S. Alfawaz, K. Nelson, and K. Mohannak, “Information security culture: a behaviour compliance conceptual framework,” in Proceedings of the Eighth Australasian Conference on Information Security-Volume 105, 2010, pp. 47–55.

[35] N. Hayaati, M. Alwi, I. Fan, and A. H. Azni, “CONCEPTUAL STUDY TOWARDS INFORMATION SECURITY MODEL FOR E-LEARNING STAKEHOLDERS,” vol. 10, no. 16, pp. 7206–7211, 2015.

[36] A. Al Hogail, “Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study,” Int. J. Secur. Its Appl., vol. 9, no. 7, pp. 163–178, 2015.

[37] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos, “The Human Factor of Information Security: Unintentional Damage Perspective,” Procedia - Soc. Behav. Sci., vol. 147, pp. 424–428, 2014.

[38] N. H. Hassan and Z. Ismail, “A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment,” Procedia - Soc. Behav. Sci., vol. 65, pp. 1007–1012, 2012.

[39] R. M. Rashid, O. Zakaria, and N. M. Zulhemay, “the Relationship of Information Security Knowledge (Isk) and Human Factors : Challenges and Solution,” J. Theor. Appl. Inf. Technol., vol. 57, no. 1, 2013.

[40] R. van der Spek and A. Spijkervet, “Knowledge management: Dealing Intelligently with Knowledge,” Ann. Occup. Hyg., vol. 49, no. 6, p. 543, 2005.

978-1-5090-6255-3/17/$31.00 ©2017 IEEE