Information Security Culture: A Definition and A Literature Review

Areej AlHogail
Department of Information Systems
College of Computing and Information Sciences
Imam Mohammed Bin Saud University Riyadh, Saudi Arabia
alhogail@ccis.imamu.edu.sa

Dr. Abdulrahman Mirza
Department of Information Systems
College of Computing and Information Sciences, King Saud University Riyadh, Saudi Arabia
amirza@ksu.edu.sa

Abstract— **Information security culture guides how things are done in organization in regard to information security, with the aim of protecting the information assets and influencing employees' security behavior. In this paper, we review key literature on information security culture that was published in the period during 2003 - 2013. The objective was to identify the frameworks that were proposed to establish and maintain information security culture inside organizations. Moreover, other issues were investigated, such as the appropriate definition, and methodology used in this field of research. The review identified 62 papers that were published in that period (2003-2013) and were focused on information security culture in organizations as a main topic of that paper. The review draws the attention to the importance of the information security culture and the need for more investigation in the field to provide a comprehensive framework of the establishment of information security culture within organization.**

Keywords: information secuirty culture; literature review.

I. INTRODUCTION

Information is one of the most valuable assets to any organisation [1] and protecting the capital of information becomes crucial to ensure a stable economy. Information breaches cost organizations Billions including the costs of data clean up, loss of data, liability and loss of customer confidence. One of the major threats to achieving a secure environment for information assets in an organization is the actions and behavior of employees when handling information [2]. A recent data breach study indicates that insiders could be behind many breaches, whether intentionally or unintentionally [3]. A number of similar studies conclude that insiders pose a threat to the protection of information [4]–[7].

Numerous surveys continue to suggest that peoples' attitudes and lack of awareness of security issues are amongst the most significant contributors to security incidents [8]. A survey conducted by PWC (Price Waterhouse Coopers) in 2013 indicated that human error, and not technology, is behind most of security breaches. The solution would be to create a security aware culture where staff should be made more aware of the risks and of their responsibilities, thereby enabling them to act in a sensible and secure manner [6]. An information security-aware culture will minimize risks to information assets and will reduce the risk of employee misbehavior and harmful interaction with the organization's information assets [6]

Von Solms [9] noted that various information security controls can only be managed properly if a comprehensive information security culture is in place, where employees know, understand, and accept the necessary precautions. Therefore, an organization should pay efforts towards building an information security culture and to integrate information security practices into its corporate culture to ensure that employees have the required knowledge and skills to act appropriately [8] and pursue a "secure" course of action. Information security culture is defined as the way things are done in the organization in order to protect information assets [6]. Recently, information security culture is increasingly considered as a way for embedding appropriate security practices in organizations [10]. Many researchers have addressed the importance and the need for an information security culture inside organizations to manage security risks to information assets, for instance, [2], [6], [11], [12].

This paper aims at formulating an understanding of the concept of information security culture. Firstly, it explores the literature in order to provide a definition of the information security culture which will serve as a reference of understanding. Then it investigates and reviews the key literature in information security culture that were published during the period (2003-2013) to identify frameworks that discuses various issues of information security culture, methodologies and empirical data used in all papers published in that period in order to help researchers in selecting the most appropriate methodology.

II. UNDERSTANDING INFORMATION SECURITY CULTURE

In order to formulate the understanding of the concept of the information security culture, this section will first highlight the concept of organizational culture to give the basis of discussion and establish the focus for the topic of information security culture. Then it will discuss the appropriate definition for information security culture

978-1-4799-3351-8/14/$31.00 ©2014 IEEE

A. *Linking information security culture to organizational culture*

Information security culture is assumed to be a part of the organizational culture as information security has become an organizational function. Information security culture is a subculture of the organization that supports all activities in a way, that information security becomes a natural aspect in the daily activities of every employee [13]. The local organizational culture will highly affect the formulation of the information security culture [10].

To achieve a secure environment for information assets, information security practices should become part of the corporate culture of an organization. The corporate culture guides the activities of the organization and its employees by placing constraints upon the activities and behavior of employees and by prescribing what the organization and its employees must, can, or cannot do [14]. The organization culture influences employee behavior, therefore, it should be used to establish the information security behavior of employees.

A number of studies in the literature have discussed the relationship between organizational culture and the information security culture. For instance, Ashenden [15] studied the challenges facing information security culture from an organizational perspective. Chang and Lin [16] presented a model of the relationship between organizational culture and ISM, that quantifies the impacts of organizational culture traits on the effectiveness of information security culture. Lim et al. [17], [18] have presented a framework to assist organizations in determining the extent to which the desired information security culture is embedded into organizational culture. Moreover, Ruighaver et al.[11] have discussed the effect of eight dimensions of organizational culture on information security culture. Findings from these studies indicate that organizational culture has a major impact on both information security management and organizational security performance.

B. *Definition of information security culture*

The concept of information security culture is relatively new [11], [19]. It was not until the start of this century that researchers first began to recognize that an information security culture might be an important factor in maintaining an adequate level of information systems security in the organizations [11], [20]. During November 2000, the Information Security Forum (ISF 2000) released a report discussing the definition of information security culture and the factors on which to focus on when measuring it. They concluded that there is a lack of a strong information security culture in organizations and literature.

In fact, information security culture is explained often using a mixture of theories and principles from other research areas due to the fact that the field of information security culture is still emerging; consequently making use of other theories as a basis for research appears logical [21]. Oost & Chew [19]argues that the variety of approaches is not a problem in itself, as it may lead to new insights to the concept.

Researchers define information security culture in different ways. Some researchers such as [13], [14], [20], [22] see information security culture as a goal to be achieved by the creation of a culture that should support all activities in a way that information security becomes a natural aspect in the daily activities of every employee job. Ngo et al.[21] and Martins & Eloff [23] see information security culture as how things are done by employees and the organization as a whole to be naturally consistent with information security principles.

Martins & Eloff [23] defines the information security culture as the perceptions, attitudes and assumptions that are accepted and encouraged by the employees in an organization in relation to information security. It is the way in which things are done in an organization to protect information assets [6]. Information security culture develops as a result of employees' interaction with information security controls [24] such as passwords, access cards or anti-virus software. Information Security Culture includes all socio-cultural measures that support technical security methods in order for making information security a natural aspect of employees' daily activities [25]. Schlienger & Teufel [25] used the definition of corporate culture as defined by Schein (1985).

Moreover, Ngo et al. [21] suggested that information security culture is the accepted behavior and actions by employees and the organization as a whole, and how things are done, in relation to information security. Information security culture involves identifying the security related ideas, beliefs and values of the group, which shape and guide security-related behaviors [26]. Malcolmson [27] argued that "Security culture is indicated in the assumptions, values, attitudes and beliefs, held by members of an organization, and behaviors they perform, which could potentially impact the security of that organization, and that may, or may not, have an explicit, known, link to that impact".

Dhillon [28] defines information security culture as "the totality of human attributes such as behaviors, attitudes, and values that contribute to the protection of all kinds of information in a given organization." Moreover, Da Veiga & Eloff [6] defined information security culture as "the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior (i.e. incidents) evident in artifacts and creations that become part of the way things are done in the organization to protect its information assets. This information security culture changes over time" p. 198. Furthermore, AlSabbagh et al.[29] suggested that information security culture is "The way our minds are programmed that will create different patterns of thinking, feeling and actions for providing the security process".

Therefore, information security culture could be defined as:

The collection of perceptions, attitudes, values , assumptions and knowledge that guides how things are done in 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.

III. REVIEW OF THE LITERATURE IN INFORMATION SECURITY CULTURE

A. Methodology

The literature about information security culture has been collected and reviewed in a systematic process that follows a qualitative content analysis. Qualitative content analysis applies a subjective interpretation of content of text through the systematic classification process of coding to identify themes or patterns.

The search process was conducted through searching the contents of on-line electronic databases, including: Google scholar, IEEE/IEE Electronic Library, EBSCOhost, Elsevier Science Direct, and Emerald Library. The search was for articles published in a 10 years period (2003-2013) using search terms that included information security culture as a keyword. Furthermore, a manual search of references cited by all returned papers has been performed to supplement the search. A context analysis has been then performed on all identified papers. Books, magazine and reviews articles have been excluded to narrow the search. All papers have been assessed by title, abstract and then by a full text evaluation.

The review identified 62 papers that were published in the period (2003-2013) and were focused on information security culture in organizations as a main topic of that paper. The review focused on identifying frameworks presented on this domain. Also it aims at recognizing the methodology used in this type of research. Other related issues that may be useful for researchers are also extracted such as the integration of knowledge management and change management. In addition, general issues like conceptualization, applications and challenges have been noted during the review. The following text will give a summarization of the review.

B. Frameworks representing information security culture

To assist organizations in establishing an information security culture, researchers have proposed various conceptual frameworks. Although there are many efforts in research towards enculturation of information security in organization, more is needed [6], [10]. During the exhaustive literature review it was found that only 14 papers (%22 of total published papers) presented a framework.

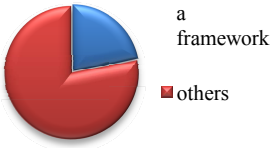
Issue investigated	No. of paper	Percentage of total papers	Representing graph
Number of papers Presented a framework for Information security culture	14	22%	

Figure 1. Analysis of papers published between (2003-2013) that presented an Information security Culture framework

The frameworks have discussed different issues in information security culture. The following text will summarize what each framework has presented.

Chia et al.[30] has adopted the organizational culture framework of Detert et al.[31]. Their work is based on information security awareness to study the effect of organizational culture on the information security culture. Their conclusion show the importance of top management support and employees' awareness and involvement. However, their paper did not provide a solution to how to improve the quality of information security culture across the organization.

Schlienger & Teufel [13] presented a framework that is based on internal marketing for analyzing the information security culture of an organization, in order to create, change and maintain information security culture. Their work is based on Schein's corporate culture model. The framework is based on five main phases: pre-evaluation, strategic planning, operative planning, implementation and post-evaluation. The process should be a cycle of evaluation, change, or maintenance.

The evaluation process includes identifying the main gap between the security policy and the perception of the employees; and identifying the areas that need improvements. The strategic planning starts with sitting a clear target culture that should be defined by the security policy. Next phase is the operative planning that includes internal communication, management buy-in, and the security awareness and training program. The implementation phase is separated in four different stages management commitment, internal communication, know-how transfer and employee commitment. Nevertheless, the model needs a practical experience to test the implementation of the proposed method and whether it can change or maintain an appropriate security culture.

Zakaria [32] presented a framework that is based on Schein's (1992) model of organizational culture. It aims at developing a data collection method in information security culture research within organization. He suggested the use of interpretive epistemology type of research. For data collection he recommends using direct observation, document review, Questionnaire and Semi-structured Interviews.

Koh et al.[33] framework examines how security governance influences security culture and in particular, the sense of responsibility and ownership of security. The authors indicate that structural and functional mechanisms in security governance are influencing factors. The authors based their framework on Chia et al. [30] framework. Authors suggested that "security governance provides adequate mechanisms to enable managers to allocate responsibilities and accountabilities for security".

The framework presented by Chang & Lin [16] examines the relationship between organizational culture and information security management (ISM) to quantify the impacts of organizational culture traits on the effectiveness of implementing ISM. The organizational culture traits include cooperativeness, innovativeness, consistency, and effectiveness. The impact is measured empirically using regression analysis. The major contribution was to stress that there are a significant relationships between organizational culture and ISM.

Dojkovski et al.[10] and [34] have presented an issue based framework for fostering an information security culture in SMEs in a national setting, namely, Australia. The authors discuss key managerial challenges in developing security culture in SMEs. They identified three external influences namely, national and ethical culture; government initiatives in raising awareness and sitting information security benchmarking; and vendors who may offer trustworthiness to SMEs. Furthermore, authors identified a number of internal influences including, governance; organizational culture that has a great affect on the information security culture; managerial factors such as security policies and procedures, and budget. In addition, individual and organizational learning including E-learning, training and education that are found to be potentially valuable initiatives for developing information security culture for SMEs. Moreover, awareness as it is essential to create and foster an affective information security culture. Also, reviewing and evaluating measures regularly to maintain the security culture. Also, behavioral factors which include a range of external and internal initiatives to create desirable security behavior.

The authors suggested that Australian SME lack management support for information security due to insufficient awareness of its importance. The authors recommend that management should be educated about the potential strategic role of information technology and information security.

Ruighaver et al. [11] used the Detert et al. [31] eight dimensions of organizational culture framework for studying an organization's security culture. In this framework, each dimension in is discussed in terms of its use to form an information security culture point of view. The ideal security culture, as authors claim, is the one that balance between both internal and external factors.

Alnatheer & Nelson [35] proposed a framework for understanding information security culture and its practices in the Saudi Arabian context. Their work focuses on the implementation and adoption processes of information security culture by identifying ISM and cultural factors and issues that assist in this regard. The aim of their framework is to investigate whether security culture has emerged into practices in Saudi Arabian organizations. According to the authors, the main factors are: corporate governance, legal and regulatory environment, and corporate citizens. Also they suggest that the security culture will be affected by the organizational culture which is affected by the national culture. However, how these factors could be used is lacking depth as they are briefly discussed.

Lim et al. [17] proposed a framework that assists organizations in determining to what extent the desired information security culture is embedded into the organization culture and exploring the nature of relationship between them. Authors argue that organizations that may have a medium to high security risk profile need to embed the information security culture into the organization in order to influence employee security behaviors and actions. Authors classify the nature of the relation to be one of three types: separated, subculture, or embedded. This framework is based on Detert et al. [31] eight dimensions organizational culture framework.

Da Veiga & Eloff [6] have proposed a framework to cultivate an information security culture within an organization that was based on a comprehensive information security framework (CISF). In their framework, they have listed a number of information security components that organizations should implement to aid in addressing human, process and technical threats that would hamper the establishment of an acceptable information security culture within the organization. The set of information security components are then grouped into categories implemented by the organization on the individual, group or organizational tier of information security behavior. So information security behavior is influenced and exhibited on each tier. The output of applying this framework is an information security culture. The framework however lacks an illustration of the possible relationships and influences between different identified components.

In the three publication, Van Niekerk & Von Solms [1], [36], [37] have discussed information security culture, through providing a model to integrate the Bloom's learning taxonomy and the use of e-learning as an educational design and delivery medium into the organizational culture change process. They have used the organizational culture levels of Schein (i.e. Artifacts, Exposed values, and Shared tacit assumptions) in their model. In addition, they have suggested that, for an effective information security culture, the required information security knowledge among employees could be seen as a fourth layer to Schein's model namely, Knowledge. The various interactions between the layers of such an information security culture were then presented conceptually.

The ideal culture would thus be one where all four underlying levels are stronger than the minimum acceptable baseline, and are also perfectly aligned relative to each other. The model also attempted to show that management demands and employees' participation are strongly interrelated. However, as authors believe that the use of the current model would only provide very vague guidance to someone wanting to manage an information security culture. In order for this model to become useful as a cultural management tool additional research would be required.

Alfawaz et al. [38] have presented a conceptual framework for classifying and organizing the characteristics of organizational subjects involved in the information security practices, by identifying how knowledge, skills and individual preferences work to influence individual and group practices with respect to information security management. Their work has focused on the influence of national and /or organizational culture. They identified four modes of behaviors: (1) Not knowing-Not doing mode, (2) Not knowing-Doing mode, (3) Knowing-Not doing mode, and (4) Knowing-Doing mode. Employee's behavior may change from one mode to another, depending on their organizational role, the state of technology development, and the status and availability of security training.

The literature analysis revealed that most frameworks have discussed different specific issues and some touched on human components such as awareness and training. However they do

not focus on the employee or on how to direct, observe and change his/her behavior [6]. In addition, most available framework are lacking a comprehensive view that integrate the human, organization and technology to provide organization with all-inclusive framework the aid organizations' information security practitioner in the implementation and adoption of information security culture.

The most comprehensive frameworks presented are Schlienger & Teufel [13] and Da Veiga & Eloff [6]. A summary of the presented frameworks is provided in Table (1).

TABLE I. SUMMARY OF PAPERS THAT PRESENTED A FRAMEWORK IN INFORMATION SECURITY CULTURE IN THE PERIOD (2003-2013)

Study	Goal of the framework presented by the study
Chia et al. (2003)	Study the effect of organizational culture on the information security culture.
Schlienger and Teufel (2003 a)	Analyzing the security culture of an organization in order to create, change and maintain Information Security Culture
Zakaria (2004)	Data collection in information security culture research
Koh et al., (2005)	Analyze how security governance influences the security culture
Chang and Lin (2007)	Quantify the impacts of organizational culture traits on the effectiveness of implementing ISM.
Ruighaver et al. (2007)	Define the concept of information security culture using Detert et al. (2000)
Dojkovski et al., (2007, 2010)	Fostering an information security culture in SMEs in a national setting.
Lim et al (2009)	Determining to what extent the information security culture is embedded into Organizational Culture.
Alnatheer and Nelson (2009)	Understanding Information Security Culture in the Saudi Context
Alfawaz et al., (2010)	Classifying and organizing the characteristics of organizational subjects involved in information security practices.
Da Veiga and Eloff (2010)	Comprehensive framework to establish information security culture.
Van Niekerk and von solms (2005;2006;2010)	Foster an information security culture in the organization through e-learning.

C. Methodologies and Data Analysis used

Out of the 62 identified papers, 29 papers (%46) had an empirical analysis that included data gathering and analysis. The remaining %54 of the papers focused on either presenting frameworks, or reviewing various information security culture issues that already present in the literature. Five proposed frameworks (around % 36 of frameworks presented) have not been supported with an empirical analysis and were based on literature review only.

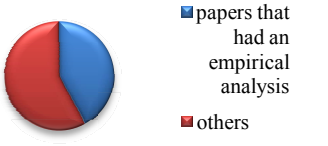
Issue investigated	No. of paper	Percentage of total papers	Representing graph
Number of papers that had an empirical analysis	29	46%	

Figure 2. Analysis of the investigation method among papers that discuss Information security culture

Different methodologies had been used; Literature review was used in %54 of the papers. In addition, interviews, survey, case studies and documents observation. Case study has been applied in 11 papers (%18 of total papers). Moreover, %14 of total papers has used interviews and %19 of the papers has used survey method. In addition, observation has been noted in 4 papers.

Some papers had combined more than one methodology together. 7 papers have used more than one methodology together, whereas the remaining papers have used only one method. Table II summarizes the survey of the methods used in the papers about the information security culture.

TABLE II. SUMMARY OF THE SURVEY OF THE METHODS USED IN THE PAPERS ABOUT THE INFORMATION SECURITY CULTURE.

Methodology used	Percentage of total papers	No. of papers
Literature review	54%	33
Case study	18%	29
Interviews	14%	11
Survey	19%	9
Observation	6%	12
interviews and case studies	5%	4
interviews, survey and documents observation	3%	3
interviews, survey, and case study	1.60%	2
interview, case studies and survey	1.60%	1
Have used only one methodology	32%	1

D. General review

Ramachandran et al. (2008) noticed that conceptualization of information security culture follows one of two paths. Firstly, scholars, such as Schlienger & Teufel (2003a)and Zakaria & Gani. A. (2003) who attempt to map the conceptualization of security culture to existing models of organizational culture (e.g., Schein's model). Secondly, scholars propose dimensions of security culture based on frameworks from the management and industrial psychology.

Moreover, Ngo et al. (2005) have noticed that research in the area of information security culture falls under two main areas: firstly, defining information security culture and the second is institutionalizing information security culture, which includes three main processes; namely establishing, fostering and managing information security culture.

Establishing a security culture means to change the current culture to a more security conscious one. This may involve altering the behavior and attitudes of people to be security aware. This may also involve an examination of the current culture in the organization to highlight areas that require greatest attention for change [21]. Research on establishing a security conscious culture include the work of [6], [22], [40], [41].

Fostering information security culture is about how to maintain information security culture to the required level after the establishment phase. As the information security culture emerges over time, managing information security culture will ensure that it will become evident in the behavior and activities of the workforce [42]. Information security behavior that is

sustained over time would evolve into an information security culture that is evident in artifacts, as well as in the values and assumptions of employees of the organization [6]. Organizations need to constantly measure and report on the state of their information security culture [6]. The work of [25] focused on managing information security culture by presenting an information security culture management cycle adapted from an internal marketing concept. The authors state that security culture is very similar to internal marketing in terms of promoting certain values, corporate goals and philosophies within an organization.

Alfawaz et al. (2010) studied a user's security behavior and suggested that by strengthening security culture of organizations' members, a significant security gains could be achieved. The effect implementation of information security culture can lead an employee to act as a "human firewall" that can safeguard organizational information assets. [10] have suggested that a strong information security culture in organizations may deal with many of the behavioral issues that cause information security breaches in such organizations.

IV. Discussions & Conclusions

In this paper we conducted an intensive review for journal and conference papers that are published during the period (2003-2013) in the field of information security culture. We identified only 62 papers published during the ten years period. The survey concludes that published research has generated a number of useful insights. It draws the attention to the importance of the information security culture. In addition, it discusses the conceptualization, application, challenges of the implementation of information security culture. This paper aims at formulating an understanding of the concept of the information security culture and to provide the summary of the literature to aid researchers wanting to investigate in this field.

The survey noted that by strengthening security culture of an organization's members, significant security gains are achieved. It leads employees to act as a "human firewall" that can safeguard organizational information assets and deal with many of the behavioral issues that cause information security breaches in organizations.

Different methodologies have been used in the reviewed paper. However, only %46 of the papers had an empirical analysis that included data gathering and analysis. The remaining %54 of papers has used literature review only. Case study, survey, interviews and document observation were the usual methods used for data collection in the reviewed papers. These figures show the need for more empirical investigations of the information security culture frameworks and issues.

Many studies mentioned that there is a need for a change management programme to be designed for assisting employees with the transition and to accept the new working procedures. This undoubtedly demonstrates the need for incorporating change management principles in order to be used to build a sound information security culture. We concluded that there is a need for more investigation in the field to provide a comprehensive framework and best practices of the establishment of information security culture within organization.

Acknowledgment

I would like to thank Dr. Saad Bakry for his valuable comments and feedback.

References

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

[2] I. Okere, J. van Niekerk, and M. Carroll, "Assessing information security culture: A critical analysis of current approaches," in *in the proceedings of IEEE conference on Information Security for South Africa (ISSA)*, 2012, pp. 1 – 8.

[3] Verizon, "Data breach investigations report 2012," 2012. [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf. [Accessed: 15-Dec-2013].

[4] J. Stanton, K. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Comput. Secur.*, vol. 24, no. 2, pp. 124–133, 2005.

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

[6] A. Da Veiga and J. Eloff, "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, Mar. 2010.

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

[8] S. Furnell, "IFIP workshop – Information security culture," *Comput. Secur.*, vol. 26, no. 1, p. 35, Feb. 2007.

[9] B. von Solms, "Information Security – The Fourth Wave?," *Comput. Secur.*, vol. 25, no. 3, pp. 165–168, 2006.

[10] S. Dojkovski, S. Lichtenstein, and M. Warren, "Fostering information security culture in small and medium size enterprises: an interpretive study in Australia," in *Proceedings of the 15th European Conference on Information Systems, University of St. Gallen*, 2007, pp. 1560–1571.

[11] A. Ruighaver, S. Maynard, and S. Chang, "Organisational security culture: Extending the end-user perspective," *Comput. Secur.*, vol. 26, no. 1, pp. 56–62, Feb. 2007.

[12] O. Zakaria, "Internalisation of Information Security Culture amongst Employees through Basic Security Knowledge," in in *IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments,*, S. Fischer-Hubner, K. Rannenberg, L. Yngstrom, and S. Lindskog, Eds. Boston: Springer, 2006, pp. 437–441.

[13] T. Schlienger and S. Teufel, "Information security culture: from analysis to change," *South African Comput. J.*, vol. 31, pp. 46–52, 2003.

[14] K. Thomson, R. von Solms, and L. Louw, "Cultivating an organizational information security culture," *Comput. Fraud Secur.*, vol. 2006, no. 10, pp. 7–11, 2006.

[15] D. Ashenden, "Information Security Management: A Human Challenge?," *Inf. Secur. Tech. Rep.*, vol. 13, no. 4, pp. 195–201, 2009.

[16] S. Chang and C. Lin, "Exploring organizational culture for information security management," *Ind. Manag. Data Syst.*, vol. 107, no. 3, pp. 438–458, 2007.

[17] 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, pp. 88–79.

[18] J. Lim, S. Chang, S. Maynard, and A. Ahmad, "Embedding information security culture Emerging concerns and challenges," in *PACIS 2010 Proceedings*, 2010, p. Paper 43.

[19] D. Oost and E. Chew, "Investigating the Concept of Information Security Culture," *university of Technology Sydney, School of Management*, 2007. [Online]. Available:

http://www.business.uts.edu.au/management/workingpapers/files/Oost2007.pdf. [Accessed: 10-Apr-2012].
[20] B. Von Solms, “Information Security – The Third Wave?,” *Comput. Secur.*, vol. 19, no. 7, pp. 615–620, 2000.
[21] 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.
[22] C. Vroom and R. Von Solms, “Towards information security behavioural compliance,” *Comput. Secur.*, vol. 23, no. 3, pp. 191–198, May 2004.
[23] A. Martins and J. Eloff, “Information security culture,” in in *Security in the information society*, Boston: Kluwer Academic Publishers, 2002, pp. 203–214.
[24] A. Martins and J. Eloff, “Assessing Information Security Culture.,” in *Proceedings of the ISSA 2002 Information for Security for South-Africa 2nd Annual Conference, 10-12 July 2002*, 2002, pp. 1–14.
[25] T. Schlienger and S. Teufel, “Analyzing Information Security Culture□: Increased Trust by an Appropriate Information Security Culture,” in *the Proceedings of the 14th International Workshop on Database and Expert Systems Applications*, 2003, p. 40.
[26] S. Ramachandran, S. Rao, and T. Goles, “Information Security Cultures of Four Professions: A Comparative Study,” in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, 2008, pp. 454–454.
[27] J. Malcolmson, “What is Security Culture? Does it differ in content from general Organisational Culture?,” in *the proceedings of the 43rd Annual International Carnahan Conference on Security Technology*, 2009, pp. 361 – 366.
[28] G. Dhillon, *Principles of information systems security*. John Wiley & Sons., 2007.
[29] B. AlSabbagh, M. AlAmeen, T. Watterstam, and S. Kowalski, “A prototype For HI2Ping information security culture and awareness training,” in *Proceedings of International Conference on e-Learning and e-Technologies in Education (ICEEE)*, 2012, pp. 32–36.
[30] P. Chia, S. Maynard, and A. Ruighaver, “Understanding organizational security culture,” in in *Information systems: the challenges of theory and practice*, Hunter M. and Dhanda K, Eds. Las Vegas, USA: Information Institute, 2003, pp. 335–365.
[31] J. Detert, R. Schroeder, and J. Mauriel, “A FRAMEWORK FOR LINKING CULTURE AND IMPROVEMENT INITIATIVES IN ORGANIZATIONS.,” *Acad. Manag. Rev.*, vol. 25, no. 4, pp. 850–863, Oct. 2000.
[32] O. Zakaria, “Understanding Challenges of Information Security Culture: A Methodological Issue.,” *AISM*, 2004.
[33] 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.
[34] S. Dojkovski, S. Lichtenstein, and M. Warren, “Enabling information security culture□: influences and challenges for Australian SMEs,” in *ACIS 2010□: Proceedings of the 21st Australasian Conference on Information Systems, ACIS*, 2010, p. 61.
[35] M. Alnatheer and K. Nelson, “A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context,” in *Proceedings of the 7th Australian Information Security Management Conference, December 2009*, 2009, pp. 6–17.
[36] J. Van Niekerk and R. Von Solms, “A holistic framework for the fostering of an information security sub-culture in organizations,” in *4th Annual ISSA Conference*, 2005.
[37] J. Van Niekerk and R. Von Solms, “Understanding Information Security Culture: A Conceptual Framework.,” in *Information Security South Africa (ISSA)*, 2006.
[38] S. Alfawaz, K. Nelson, and K. Mohannak, “Information security culture: a behaviour compliance conceptual framework,” in *8th Australasian Information Security Conference (AISC 2010)*, 2010, pp. 47–55.
[39] O. Zakaria and Gani. A., “A Conceptual Checklist Of Information Security Culture,” in *Proceedings of 2nd European Conference on Information Warfare and Security*, 2003.
[40] L. Drevin, H. Kruger, and T. Steyn, “Value-focused assessment of {ICT} security awareness in an academic environment,” *Comput. Secur.*, vol. 26, no. 1, pp. 36–43, 2007.
[41] I. Koskosas, K. Kakoulidis, and C. Siomos, “Information Security: Corporate Culture and Organizational Commitment,” *Int. J. Humanit. Soc. Sci.*, vol. 1, no. 3, pp. 192–198, 2011.
[42] A. Da Veiga, N. Martins, and J. Eloff, “Information security culture-validation of an assessment instrument,” *South. African Bus. Rev.*, vol. 11, no. 1, pp. 146–166, 2007.