A Conceptual Model to Understand Information Security Culture

Mohammed A. Alnatheer

***Abstract*—The purpose of the paper is to examine the conceptualization of information security culture in order to develop an information security culture measurement model. In order to do so, a comprehensive literature analysis of current information security culture models and frameworks were examined. The outcome of the comprehensive review is a top constructs candidate that conceptualizes security culture. The current paper found no mutual agreement on what factors conceptualize a security culture. Our contribution is being able to identify a clear gap on the existing literature of a lack of clear conceptualization and distinction between factors that *constitute* information security culture and factors that *influence* information security culture. The distinction clearly has not been made by academic literature on the information security culture. The current study assists academic researchers to identify research gaps in the information security culture field, including identifying further empirical research needed in this area.**

***Index Terms*—Security culture, factors constitute security culture, factors influence security culture.**

I. Introduction

The purpose of this paper is to provide an understanding of information security culture through developing information security culture conceptual model. This paper first provides a brief introduction to information security culture. Then, the development and production of the conceptual model was based on a comprehensive review of academic and professional literature on information security cultural areas was examined. This paper will be finalized by identifying the conceptual model that includes a set of candidate factors that conceptualize security culture models. Some of the current definitions found for security culture are:

Information security culture can be defined as: The information security perceptions, attitudes and assumptions those are accepted and encouraged in an organisation – thus the way in which things are done in an organisation to protect information assets [1] (p.148).

A more extensive definition for information security culture as:

An information security culture is defined 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 procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artefacts and creations that become part of the way things are done in an organization to protect its information assets [2] (p.26). This information security culture changes over time.

Information security culture is a subculture in regards to content. Security culture encompasses all socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee [3] (p.405).

Security culture can also be defined as: The totality of patterns of behaviours in an organization that contribute to the protection of information of all kinds [4] (p.90).

In [5] (p.618) calls for security culture creation within organization: By instilling the aspects of information security to every employee as a natural way of performing his or her daily job.

The same author (p.616) added that:

corporate information security culture that supports the information security policies, procedures, methods and responsibilities of the company, in such a way that information security becomes a natural aspect of the day to day activities of all employees of the company.

Security culture can be referred as: How things are done (i.e. accepted behaviour and actions) by employees and the organisation as a whole, in relation to information security [6] (p.68).

Information security culture can be discussed as:

- A set of information security characteristics that the organisation values,
- The assumption about what is acceptable and what is not in relation to information security,
- The assumption about what information security behaviour is encouraged and what is not,
- The way people behave towards information security in the organisation [7] (p.204-205).

Despite the importance of the previous definitions, in recognising the need to create security culture in order to manage security effectively, these definitions, only focuses on the manifestation of information security culture within organizations. They define what security culture is-it reflects values, behaviour, beliefs, altitude and action of the organizations members. These definitions did not specifically discussed what factors or constructs that constitute or conceptualized information security culture. Most of the current information security culture researches had applied theories from different perspective: from organization culture [8]; organization behaviour [9]; total quality management [10]; and as part of national culture [11]. Some of the existing literature has adopted Schein organizational culture model to study information security culture [3], [9], [12]. These studies indicated that all of the information security elements and

Manuscript received July 1, 2013; revised September 5, 2013.

Mohammed A. Alnatheer is with the King Abdul-Aziz City for Science and Technology, Riyadh, Saudi Arabia (e-mail: mnatheer@kacst.edu.sa).

issues can be represented in the three levels of the organizations culture model (artefacts, values and assumptions). These studies indicated information security culture is a product of different factors in which influence the behaviour of individual within the organization settings.

II. Development of Conceptual Model

In order to develop a reliable and valid information security culture measurement model, an understanding of current information security culture existing models and frameworks is essential. As a result, a comprehensive review of information security culture models and frameworks was conducted and used as a foundation for developing conceptual model. The first purpose of the comprehensive review is to identify and examine the conceptualizations of information security culture. The second purpose of this comprehensive review is to provide a detailed list and analysis of constructs that were proposed by each study in the information security culture area in order to develop the conceptual model. This review has also focused on studies that included a questionnaire instrument that assesses information security culture to assist in developing an information security culture measurement model.

TABLE I: Summary of Current Proposed Constructs in Information Security Culture Research

Research	Constructs/ Findings
[7]	Security policy; Change management; Risk analysis; Benchmarking; Budget; Trust; Awareness; Ethical Conduct
[13]	**Leadership and governance** Sponsorship; Strategy; IT Governance; Risk Assessment; ROI / Metrics /Measurement **Security management and organisation** Program Organization; Legal & Regulatory **Security policies** Policies; Procedures; Standards; Guidelines; Certifications; Best practice **Security program management** Monitoring and Audit; Compliance **User security management** User Awareness; Education and Training; Ethical Conduct; Trust; Privacy **Technology protection and operations** Asset Management; System Development; Incident Management; Technical operations; Physical and environmental; Business Continuity **Change:** Change Management
[14], [15]	**Schein organisational culture model: Security culture has three layers:** **Corporate Politics that include:** Security policy; Organization structure; Resources **Management that includes:** Implementation of security policy; Responsibilities; Qualification and training; Awards and prosecutions; Audits; Benchmarks; **Individual that includes:** Attitude; Communication, compliance
[16], [17]	**Security culture Framework:** Standardization; Certification; Measurement of information security **Content components:** People's attitude; Motivation; Knowledge; Communication, compliance
[18]	Awareness; Responsibility; Response; Ethics; Democracy; Risk assessment; Security design and implementation; Security management; Reassessment
[19]	**Managerial aspect** Policies and procedures; Benchmarking; Risk analysis; Budget; Management response; Training and Education; Awareness; Change management **Behaviour Issues** Responsibility; Integrity; Trust; Ethnicity; Values; Motivation; Orientation **Individual and Organization e-learning** Training and Education **Ethical; National culture; Organization culture**
[20]	Employee Participation; Training; Hiring Practices; Reward System; Management Commitment; Communication and Feedback
[21]	Security budget; Security expenditure; Employee security awareness; Security risk of staff; Implementing the security policy; Making security suggestions; Security Ownership; Security Audits
[22]	Security Awareness; security ownership; Security Risk; Compliance with security rules and regulations
[23]	**Management:** Policies; Personnel; Training; Education; **Principles and values:** Responsibility; Honesty; Integrity; Ethics; Commitment; Compliance; Leadership; Motivations **Shared underlying assumptions:** Knowledge; Trust relationships; Beliefs
[24]	Security Governance Framework: Structural Mechanisms; Functional Mechanisms; Social Participation; **Influences on** Security Culture Framework Dimension particularly: Control; Coordination; Ownership
[25],[26]	Top management; Policy change; Effective Information Security; Education program

The main reason for focusing on studies that include a questionnaires instrument because it will assist this study in developing a reliable a valid an information security culture measurement model instruments. Important criteria in the literature review evaluation process include: development of the assessment instrument, content validity, construct validity and reliability. These criteria will assist in identifying: firstly, the existing gap in the information security culture literature; and secondly, a valid and reliable information security measurement. The findings of this review indicated there are only two out of the thirteen information security culture research models that have provided a validated information security culture assessment instrument [3], [13]. In the first of these, an instrument was developed by Da Veiga, and Eloff (2009) designed to cultivate information security culture. In the second, Schlienger and Teufel (2003) designed a questionnaire to obtain an understanding of official rules intended to influence the security behaviour of employees. While [7] have developed a theoretical information security culture framework to assess information security culture, they did not validate their questionnaires. Other information security culture research provide proposed constructs to develop a security culture framework but did not develop an assessment instrument to measure information security culture. These researches, however, have one distinguish limitation. They did not clearly distinguish between factors that *constitute* information security culture and factors that *drive* information security culture within the organization settings.

Table I summarizes the list of information security culture research constructs for each study. The first column of the Table I represents various information security culture research frameworks. The second columns represents constructs and findings for each relative information security culture frameworks.

Thirteen studies were retrieved in Table I. The process used to develop the conceptual model was to extract research in existing information security culture frameworks and models in order to develop an understanding of current information security culture phenomena. For each study, all the proposed constructs were extracted and counted in Table II. The purpose for counting constructs for each study is to identify top constructs as potential candidates because it is simply impossible to examine every factor that could help conceptualize a security culture. Most of the literature examined the creation of security culture broadly. There is simply no mutual agreement on what factors constitute a security culture. In other words, there is a clear gap in terms of identifying factors that help conceptualize a security culture. As a result, the conceptualizations of security culture will be the focus part of this paper. Because of the scope limitation, the current paper will only consider the top constructs where there is strong agreement between academic researchers as to their importance for security culture adoption. Table II presents top candidate constructs for conceptualizing a security culture**.** The current study extracted the top seven constructs as candidate constructs of interest for the conceptual model. These factors are:

Top Management Support for Information Security,

- Establishing an Effective Information Security Policy through Policy Enforcement,
- Security Awareness,
- Information Security Training,
- Information Security Risk Analysis and Assessment,
- Security Compliance,
- Ethical Conduct Policies

Additionally, it is essential to examine external cultural factors surrounds the adoption or creation of security culture. These factors are mainly organizational and national culture. Organization culture has emerged in this literature review as essential elements that influence security culture. Security culture was itself considered as part of the organization culture [10], [15], [19]. Moreover, national culture is known to have cultural beliefs in which have strong influences on Information Technology diffusion [27]. Therefore, the national culture might be able to influence security culture in worldwide organisations. Additionally, Chaula, (2006) studies has considered security culture as part of national culture in the developing countries context. As a result, national culture will be a candidate among the external factors that influence security culture.

TABLE II: CONSTRUCTS OF INTEREST APPEAR IN THE INFORMATION SECURITY CULTURE RESEARCH

Constructs	Number of Times Cited out of 13 studies	Construct Rankings
Management commitment to Information Security	8/13	1
Security policy and policy enforcement	6/13	2
Security Awareness	6/13	2
Security training and education	6/13	2
Security Risk assessment	6/13	2
Security Compliance	5/13	6
Ethical Conduct	5/13	6

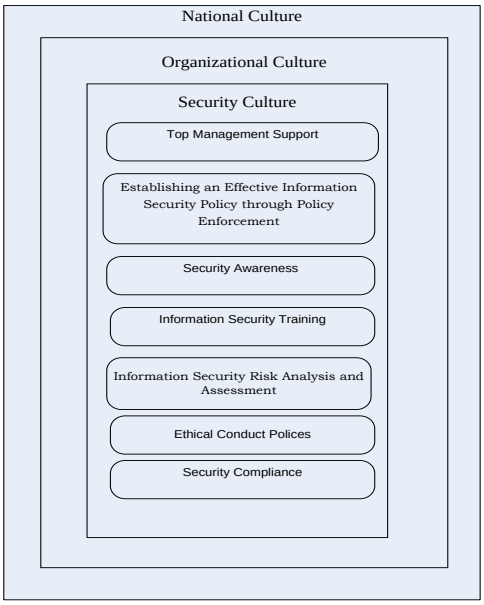

Fig. 1. Conceptual model development.

As illustrated in Fig. 1, security culture is embedded part of organization and organization culture embedded part of

national culture. National and organizational culture could have strong influence on security culture adoption and will be part of the research conceptual model.

III. Discussion and Future Work

This review of the information security culture research area illustrates the lack of empirical measurement in the information security culture area. The existing literature has emphasized the importance of information security culture and provided suggestions and guidelines on how to assess information security culture. These literature analyses have not provided a clear understanding of how security culture must be conceptualized in order for researchers to develop an instrument for the understanding and measurement of an information security culture model. Furthermore, there is little clarification as to what exact factors constitute security culture and as to what factors influence or drive the creation of security culture. The distinction clearly has not been made by academic literature on the information security culture. In other words, there is a clear gap in knowledge in terms of identifying what factors constitute or reflect the security culture and what factors influence the security culture. Therefore, the current study will take this initiative and develop an information security culture measurement model that clearly distinguishes between what factors constitute security culture and what factors influence or drive the security culture. In order to achieve this goal, an open ended interview will be implemented to develop the information security culture measurement model in organisations. Additionally, the qualitative interviews will also assist in minimizing subjectivity in identifying factors for the research conceptual model. However, other factors could emerge after conducting and analysing the qualitative interviews. The qualitative interviews would be the future work of our paper.

References

[1] A. D. Veiga., N. Martins, and J. Eloff, "Information security culture–validation of an assessment instrument," *Southern African Business Review*, vol. 11, no. 1, pp. 146-166, 2007.

[2] A. D. Veiga, "Cultivating and assessing information security culture," PhD. Dissertation, University of Pretoria, 2008.

[3] T. Schlienger and S. Teufel, "Analyzing information security culture: increased trust by an appropriate information security culture," in *Proc.14th International Workshop on Database and Expert Systems Applications (DEXA'03)*, 2003.

[4] G. Dhillon, "Managing and controlling computer misuse," *Information Management & Computer Security*, vol. 7, no. 4, pp. 171-175, 1999.

[5] S. V. Solms, "Information Security-The Third Wave?" *Computer & Security*, vol. 19, pp. 615-620, 2002.

[6] L. Ngo, W. Zhou, and M. Warre, "Understanding transition towards information security culture change," in *Proc. Third Australian Information Security Management Conference*, Perth, Australia, pp. 67-73, 2005.

[7] A. Martins and J. Eloff, "Information Security Culture," in *Proc.* 17th *International Conference on Information Security*, Cairo, Egypt, 2002.

[8] S. Chang and C. Lin. "Exploring organisational culture for information security management," *Industrial Management & Data Systems*, vol. 107, no. 3, pp. 438-458, 2007.

[9] K. Thomson and R. von Solms, "Information security obedience: A definition," *Computers & Security*, vol. 24, pp. 69-75, 2005.

[10] P. Chia, S. Maynard, and A. Ruighaver, "Understanding organisational security culture," in *Information Systems: The Challenges of Theory and Practice*," M. Hunter and M. Dhanda, Eds. Las Vegas, USA: Information Institute, 2003, pp. 335-365.

[11] A. Chaula, "A socio-technical analysis of information systems security assurance: A case study for effective assurance," PhD. Dissertation, Stockholm University, Stockholm, 1993.

[12] O. Zakaria, "Understanding challenges of information security culture: a methodological approach issue," in *Proc. 5th* 2nd *Australian information Security Management Conference*, Perth, Australia, 2004.

[13] A. Da Veiga and, J. Eloff, "A framework and assessment instrument for information security culture," *Computer & Security*, pp. 1-12, 2009.

[14] T. Schlienger and S. Teufel, "Information security culture: the socio-cultural dimension in information security management," in *Proc. Security in the Information Society: Visions and Perspectives*, Kluwer, Deventer, Netherlands, pp. 191-202, 2002.

[15] T. Schlienger and S. Teufel, "Tool supported management of information security culture: An application to a Private Bank," in *Proc. 20th IFIP International Information Security Conference (SEC 2005)*, Security and Privacy in the Age of Ubiquitous Computing, Chiba, Japan, Kluwer Academic Press, 2005.

[16] T. Helokunnas and R. Kuusisto, "Information security culture in a value Net," in *Proc. 2003 IEEE International Engineering Management Conference (IEMC)*, pp. 2-4, 2003.

[17] T. Kuusisto and I. Ilvonen, "Information security culture is small and medium enterprises," *Frontier of E-business Research*, pp. 431-439, 2003.

[18] OECD, *Guidelines for the Security of Information Systems and Networks*, 2003.

[19] S. Dojkovski, S. Lichtenstein, and M. J. Warren, "Fostering information security culture in small and medium size enterprises: an interpretive study in Australia," in *Proc. 15th European Conference on Information Systems*, University of St. Gallen, St. Gallen, Switzerland, 2006.

[20] S. Kraemer and P. Carayon, "Computer and information security culture: findings from two studies," in *Proc. Human Factors and Ergonomics Society 49th Annual Meeting*, Orlando, United States, 2005, pp. 1483-1487.

[21] P. Chia, S. Maynard, and A. Ruighaver, "Exploring organizational security culture: Developing a comprehensive research model," in *Proc. IS ONE World Conference*, Las Vegas, Nevada USA, 2002.

[22] S. Ramachandran, V. Srinivasan, and T. Goles, "Information security cultures of four professions: a comparative study," in *Proc. 41st Hawaii International Conference on System*, Hawaii, USA, 2004.

[23] C. N. Tarimo, J. K. Bakari, L. Yngström, and S. Kowalski, "A social-technical view of ict security issues, trends, and challenges: Towards a culture of ICT security the case of Tanzania," in *Proc. Fifth Annual Information Security Conference South Africa (ISSA)*, Gauteng, South Africa, 2006.

[24] K. Koh, A. Ruighaver, S. Maynard, and A. Ahmad. "Security governance: Its impact on security culture," in *Proc. 3rd Australian Information Security Management Conference*, Perth, Australia, pp., 1-13, 2005.

[25] J. van Niekerk and R. von Solms, "A holistic framework for the fostering of an information security sub-culture in organisations," in *Proc. Annual Information Security Conference South Africa (ISSA)*, 2005.

[26] J. van Niekerk and R. von Solms, "Understanding information security culture: A conceptual framework," in *Proc. 5th Annual Information Security Conference South Africa (ISSA)*, 2006.

[27] D. Straub, K. Loch, and C. Hill, "Transfer of information technology to the Arab world: a test of cultural influence modeling," in *Advanced Topics in Global Information Management*, Hershey, PA: Idea Group Publishing, 2003, pp. 141-172.

Mohammed Alnatheer was born in the city of Ar'Ar, Saudi Arabia in July 1978. Mohammed Alnatheer Hold a bachelor of science in electrical and computer engineering in 2003 and master of science of computer science in 2004 from West Virginia University, WV, USA. Mohammed Alnatheer holds a PhD degree in information technology in 2013 from Queensland University of Technology, Brisbane, Australia. Currently, He is an assistance research professor at King Abdulaz-z City for Science and Technology in Riyadh, Saudi Arabia. Mohammed Alnatheer is conducting researches in research areas related to information security and more specifically related to information security management areas.