International Journal of Security and Its Applications
Vol. 11, No. 5 (2017), pp.15-26
http://dx.doi.org/10.14257/ijsia.2017.11.5.02

A Conceptual Model for Exploring the Factors Influencing Information Security Culture

Amjad Mahfuth[1]*, Salman Yussof[2], Asmidar abu bakar[3], Nor'ashikin Bte. Ali[4] and Waleed Abdallah[5]

[1,5]College of Technology and Applied Science, Al-Quds Open University, Jerusalem, Palestine
[2,3,4] College of Computer Science and Information Technology, Universiti Tenaga Nasional, Putrajaya, Malaysia
[1]amahfouz@qou.edu, [2]Salman@uniten.edu.my, [3]Asmidar@uniten.edu.my
[4]Shikin@uniten.edu.my, [5]wsalos@qou.edu

Abstract

Human behavior is considered as one of the main threats in an organization. Owing to the fact that human element is the weakest link in security area, it is crucial to provide an ideal information security culture within an organization in order to guide the employees' perception, attitudes and security behavior. Furthermore, this culture can protect an organization against many information security threats posed by the employees. In this paper, we have proposed a conceptual model exploring the factors influencing the information security culture. Those factors are Security Awareness, Security Knowledge, Belief, Top Management, Security Policy, Security Behavior , Information Security Training, Security Risk Analysis and Assessment, Security Compliance, Ethical and Legal, Trust, Technology, Change Management, People, Information Security, Security Responsibility, Process, Strategy and Environment. The aim of the conceptual model would help the researchers to develop effective solutions and to provide a suitable background for information security culture across an organization. The study recommends researchers to conduct many studies in this area to focus on and investigate each of identified factors in the conceptual model in order to improve information security culture in organizations.

Keywords*: Information security culture, organization, factors, information security culture framework. Security behavior*

1. Introduction

Information is one of the most important factors in an organization. It is crucial to protect the valued information in order to ensure information's stability, availability, integrity and confidentiality [1, 2]. A recent study such as [3] has reported that organizations have lost billions of dollars due to information breaches. Employees, who are interacting with organization assets can be considered as the major threat leading to data breaches occurred in an organization. This finding has been supported by the standard formal statistical study [4]. This leads to a negative impact on the confidence of customers on the institution. Moreover, other studies such as [5–8] have concluded that the insiders pose many threats to the protection of the information inside an organization.

Concentrating on a technical measurement to protect the organization assets without any consideration to human factor evidently is inadequate. Human factor is the weakest link in security [2, 9, 10] Human error and his/her negligence are the common causes of data breaches that occurred in an organization [11, 12]. Therefore, an organization should focus on employees' behaviors, attitudes, assumptions and awareness in order to achieve

ISSN: 1738-9976 IJSIA

information security. Moreover, the effectiveness of an information security system relies on the actions of the employees [13]. Inculcating information security culture within an organization will minimize the risks of data breach and employees misbehavior [1, 4].

Numerous definitions of information security culture have been provided by security researchers. In [14] have defined information security culture as "The attitudes, assumptions, beliefs, values and knowledge used by the employees to interact with the organization's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior evident in artifacts and creations that become part of the way things are done in an organization to protect its information assets". In [15] have defined information security culture as "The collection of perceptions, attitudes, values, assumptions and knowledge that guides how things are done in an 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 presented by [16] is "The collection of human attributes such as behaviors, attitudes, and values that help to the protection of all the information in an organization."

Based on the presented definitions of information security culture, we can view information security culture as an integration process of perceptions, attitudes, values, assumptions and knowledge that guide, direct and manage the employees' perceptions and attitudes to influence employee 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 in an organization, whereby the organization and the employees must work closely in order to find a conducive environment for information security culture to be inculcated throughout the organization.

This paper adopts the systematic literature review (SLR) approach to provide a conceptual model exploring the factors influencing the information security culture. The SLR focused on all papers pertaining to information security culture were published during the period with in (2003-2016). Our contributions are presented in the following sections.

2. Research Method

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 electronic databases, including Google scholar, IEEE/IEE Electronic Library, Elsevier Science Direct, ACM and Springer. Reviews have been done on papers published from year 2003 to 2016 by using keywords related to information security culture. Qualitative content analysis is used to identify and classify the papers accordingly. Our search has identified 68 papers focusing on information security culture. However, the current review focuses on the frameworks, methodologies and factors affecting the information security. Upon filtering these papers based on our research goal, we have found 18 papers (27 % of total papers) that focus on information security culture framework. The other papers focus on other topics such as definitions of information security culture, key factors influencing information security culture, challenges of information security culture, relationship between the organizational culture and information security culture, cultivation process for implementing information security, general issues regarding information security culture and assessment instrument for information security culture. There are also papers that have conducted empirical studies which include data collection and analysis.

3. Results

The main objective of this paper is to answer the question: “What are the key factors influencing information security culture?”

Table (1) consolidates the key factors influencing information security culture that have been obtained from the literature. The antecedents are categorized as Security Awareness, Security Knowledge, Belief, Top management, Security Policy, Security Behavior , Information Security Training, Security Risk Analysis and assessment, Security Compliance, Ethical and Legal, Trust, Technology, Change Management, People, Information Security, Security Responsibility, Process, Strategy, and Environment. We have also proposed a conceptual model for the factors influencing information security culture as illustrated in Figure 1.

4. Discussion and Future Work

The current literature review has identified all factors which would influence the information security culture in an organization. These factors vary in terms of their importance and impacts to information security culture. From Table (1), it can be seen that information security policy and information security awareness are the two factors most proposed by researchers. This suggests that conducting security awareness programs for employees in an organization is a necessity to inculcate positive information security culture in the organization. However, for the security awareness program to be effective, the contents must properly be selected and designed. More research needs to be done in this area so that the security awareness program can produce the intended results. Once the employees of an organization is equipped with information security awareness and knowledge, the information security policy set by the organization can be more easily implemented and complied upon. Furthermore, the literature review reveals that there is a lack to investigate what is required of security knowledge that should be incorporated across the organization in order to improve information security culture.

Moreover, the literature review reveals that most of the identified factors are linked directly to information security culture without any details provided in each factor such as construct, dimension and impact to information security culture. Furthermore, limited empirical studies have been conducted to measure the impact of each factor to information security culture. In other words, there is an obvious knowledge gap in identifying each factors and measuring its impacts to security culture.

This study help the researchers to explore the factors influencing information security culture by the previous studies. In addition, it invites the researchers to perform more investigations regarding the identified factors.

Table 1. The Following Table Summarizes the Key Factors

No.	Key Factors	Studies	Number of Occurrence
1.	Security Awareness	[14];[17];[18];[19];[20];[10];[21];[22];[22];[23];[24];[25];[26];[27]	14
2.	Security Knowledge	[28]; [29]	2
3.	Belief	[30];[31]; [32]; [27]	4
4.	Top Management	[18]; [20] ;[29]; [14]; [33];[23]; [34];[35];[36];[37]	10
5.	Security Policy	[18] ;[29];[2];[10]; [14]; [33]; [22];[38];[23]; [24] ;[25];[37];[34];[35];[26];[39];[40];[27]	18
6.	Security Behavior	[14]; [33];[32];[35]; [41]	5
7.	Information Security Training	[14] ; [19]; [38];[23];[26];[39];[40];[27]	8
8.	Security Risk Analysis and Assessment	[10];[14];[23] ; [24];[27]	5
9.	Security Compliance	[14]; [38] ;[41];[39] ;[40];[27]	6
10.	Ethical and Legal	[10]; [14]; [33];[23];[42];[39]	6
11.	Trust	[27];[10]	2
12.	Technology	[14] ;[33]	2
13.	Change Management	[14];[2]; [33];[23]	4
14.	People	[14]; [33];	2
15.	Information Security Management	[37]	1
16.	Security Responsibility	[37];[27]	2
17.	Process	[14];[33]	2
18.	Strategy	[14];[33]	2
19.	Environment	[33]	1

Based on Figure 1, we can hypothesize the followings:
H1: Security Awareness has a positive relation with information security culture.
H2: Security Knowledge has a positive relation with information security culture.
H3: Belief has a positive relation with information security culture.
H4: Top Management has a positive relation with information security culture.
H5: Security Policy has a positive relation with information security culture.
H6: Security Behavior has a positive relation with information security culture.
H7: Information Security Training has a positive relation with information security culture.
H8: Security Risk Analysis and Assessment has a positive relation with information security culture.
H9: Security Compliance has a positive relation with information security culture.
H10: Ethical and legal have positive relations with information security culture.
H11: Trust has a positive relation with information security culture.

H12: Technology has a positive relation with information security culture.
H13: Change Management has a positive relation with information security culture.
H14: People (The Employees) have a positive relation with information security culture.
H15: Information Security Management has a positive relation with information security culture.
H16: Security Responsibility has a positive relation with information security culture.
H17: Process has a positive relation with information security culture.
H18: Strategy Security Awareness has a positive relation with information security culture.
H19: Environment has a positive relation with information security culture.

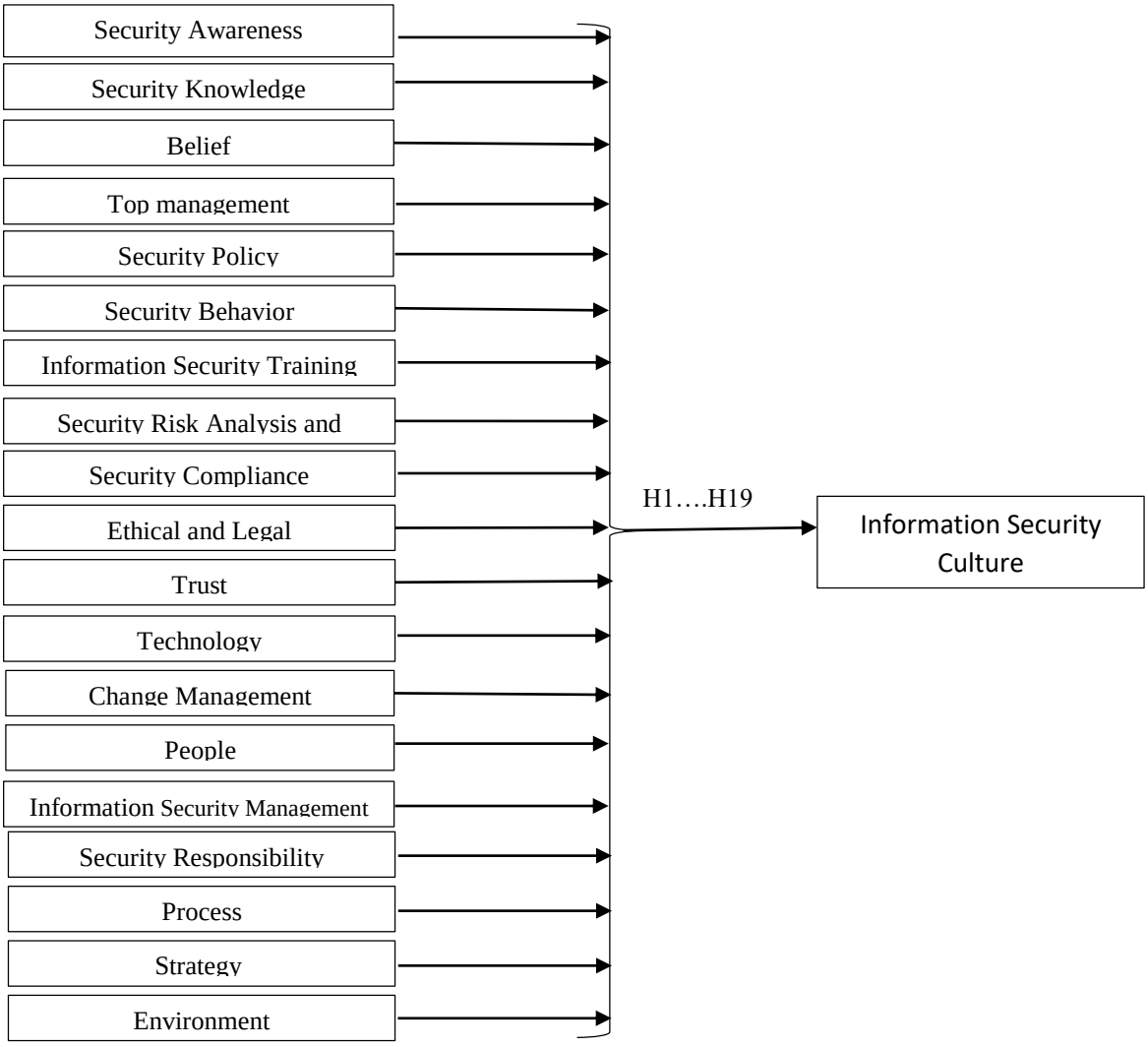

Figure 1. A Conceptual Model for the Factors Influencing Information Security Culture

6. Conclusion

In this paper we have conducted a systematic literature review focusing on the information security culture. A total of 19 factors influencing the information security culture have been identified. Moreover, the current work reveals the importance of implementing information security culture in an organization in order to minimize

information/data breach. Finally, In order to measure the impacts of these factors on information security culture, further studies must be performed.

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] 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.
[3] Ponemon Institute, "2015 Cost of Data BreachSstudy: Global Analysis," no. May, pp. 1–30, 2015.
[4] Verizon, "2014 Data Breach Investigations Report," Verizon Bus. J., vol. 2014, no. 1, pp. 1–60, 2014.
[5] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," Comput. Secur., vol. 24, no. 2, pp. 124–133, 2005.
[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 and J. H. P. Eloff, "A framework and assessment instrument for information security culture," Comput. Secur., vol. 29, no. 2, pp. 196–207, 2009.
[8] 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.
[9] 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.
[10] A. Martins and J. Elofe, "Information security culture," in Security in the information society, Springer, 2002, pp. 203–214.
[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] 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.
[13] 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.
[14] 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.
[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] G. Dhillon, Principles of Information Systems Security: text and cases. Wiley New York, NY, 2007.
[17] I. Al-Mayahi and P. M. Sa'ad, "Information security culture assessment: Case study," in 2013 IEEE Third International Conference on Information Science and Technology (ICIST), 2013, pp. 789–792.
[18] S. E. Donahue, "Assessing the impact that organizational culture has on enterprise information security incidents," phdthesis, CAPELLA UNIVERSITY, 2011.
[19] 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.
[20] T. Gebrasilase and L. F. Lessa, "Information security culture in public hospitals: the case of Hawassa referral hospital," African J. Inf. Syst., vol. 3, no. 3, p. 1, 2011.
[21] A. Da Veiga and N. Martins, "Improving the information security culture through monitoring and implementation actions illustrated through a case study," Comput. Secur., vol. 49, pp. 162–176, 2015.
[22] H. Shaaban and M. Conrad, "Democracy, culture and information security: a case study in Zanzibar.," Inf. Manag. Comput. Secur., vol. 21, no. 3, pp. 191–201, 2013.
[23] 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.
[24] P. a. Chia, S. B. Maynard, and a. B. Ruighaver, "Understanding Organizational Security Culture," Pacis, pp. 1–23, 2002.
[25] 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.
[26] Y. A. N. Chen, K. R. A. M. Ramamurthy, and K. Wen, "Impacts od Comprehensive Information Security Programs on Information Security Culture," J. Comput. Inf. Syst., vol. 55, no. 3, p. 11, 2015.
[27] P. A. H. Williams, "Capturing Culture in Medical Information Security Research," Methodol. Innov. Online, vol. 4, no. 3, pp. 15–26, 2009.
[28] O. Zakaria, "Internalisation of information security culture amongst employees through basic security knowledge," IFIP Int. Fed. Inf. Process., vol. 201, pp. 437–441, 2006.
[29] J. F. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," Comput. Secur., vol. 29, no. 4, pp. 476–486, 2010.
[30] M. I. Merhi, Creating an information systems security culture through an integrated model of employees

compliance. THE UNIVERSITY OF TEXAS-PAN AMERICAN, 2014.
[31] D. Ashenden and A. Sasse, "CISOs and organisational culture: Their own worst enemy?," Comput. Secur., vol. 39, pp. 396–405, 2013.
[32] W. DOLLAH and J. ALI, "Determining factors influencing information security culture among ICT librarians," J. Theor. Appl. Inf. Technol., vol. 37, no. 1, 2012.
[33] 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.
[34] J. D'Arcy and G. Greene, "Security culture and the employment relationship as drivers of employees' security compliance," Inf. Manag. Comput. Secur., vol. 22, no. 5, pp. 474–489, 2014.
[35] 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.
[36] Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing employee compliance with information security policies: The critical role of top management and organizational culture," Decis. Sci., vol. 43, no. 4, pp. 615–660, 2012.
[37] 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.
[38] T. Schlienger and S. Teufel, "Information security culture-from analysis to change," South African Comput. J., no. 31, p. p--46, 2003.
[39] B. Al Sabbagh and S. Kowalski, "Developing social metrics for security modeling the security culture of it workers individuals (case study)," in Communications, Computers and Applications (MIC-CCA), 2012 Mosharaka International Conference on, 2012, pp. 112–118.
[40] F. Karlsson and K. Hedström, "End User Development and Information Security Culture," in Human Aspects of Information Security, Privacy, and Trust, 2014, pp. 246–257.
[41] 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.
[42] M. Alnatheer and K. Nelson, "Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context," Aust. Inf. Secur. Manag. Conf., no. December, pp. 6–17, 2009.

