ISSN 2278-3091

Volume 9, No.1.3, 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1691.32020.pdf

https://doi.org/10.30534/ijatcse/2020/1691.32020

Information Security Culture Model for Malaysian Organizations: A Review

Akhyari Nasir[1], Ruzaini Abdullah Arshah[2], Mohd Rashid Ab Hamid[2], Syahrul Fahmy[1], MohdTamizan Abu Bakar[1]

[1]University College TATI, Malaysia, akhyari@tatiuc.edu.my

[2]Universiti Malaysia Pahang, Malaysia

ABSTRACT

The establishment of Information Security Culture (ISC) has been recommended for improving employees' information security in the organization. To date, there is still no clear guidance or model for assessing and cultivating ISC for Malaysian organizations, despite some Malaysian-based studies being carried out. In order to shed light to this issue, we reviewed all ISC models developed in Malaysian context to identify models for particular types of organization in Malaysia. Three major databases of Web of Science, Scopus and Google Scholar were systematically exhausted and we found only six papers from 2000 to 2018 that met our selection criteria. Our analysis revealed that there is a lack of validated ISC models have been produced for particular types of organization. The current model only applicable to healthcare, library and public organizations in Malaysia. In addition, there is a lack of consistency in terms of ISC factors used in the ISC models and there is no common set of factors could be applied for all type of Malaysian organization. This review has amplified the need for a more thorough and in-depth studies for ISC model in Malaysian context.

Key words: Factor, Information Security Culture, Malaysia, Model.

1. INTRODUCTION

Due to increasing number of information security incidents that caused by internal employees, scholars and experts recommended practitioners to establish a positive Information Security Culture (ISC) to guide employee's security behaviour in the organization [1-7]. Since the early of this millennium, many ISC studies have been conducted from many aspects to understand and utilize the benefits that this culture could offer. Until now, there are number of findings that could be used by academicians and practitioners in terms of knowledge and applications of ISC.

Despite these findings, there is little knowledge on how to assess or establish this culture in Malaysian organization. There is a lack of study conducted to provide a clear picture of what have been done in literature that could assists the practitioners in selecting the best ISC strategy for their organizations. Based on this motivation, we analyze all ISC studies in Malaysian organizations context to synthesize all the findings in providing a status quo of ISC model in Malaysia. Since the factors or dimensions of an ISC model are representing the aspects on how to establish ISC, the review is focussing on ISC model based on dimensions/factors. Next section discusses the methodology use in this review followed by presentation of findings in Section 3. The discussion on the findings discusses in Section 4 and limitations as well as future works discusses in Section 5. Finally, the conclusion of this review is presented in Section 6.

2. METHODOLOGY

This study utilizes the search procedure of [8] to identify and select the papers to be reviewed as shown in Figure 1. This is because the searching process in [8] has the similar objective which is to find the studies that discuss ISC model based on factors and dimensions. However, our study is focuses on studies that conducted in Malaysian organizations only. As such, the first criteria for paper selection is, the paper must discuss regarding ISC model in the context of Malaysian organization. Secondly, since this review is to identify the aspects or elements of ISC, the paper must also discuss the model based on factors or dimensions.

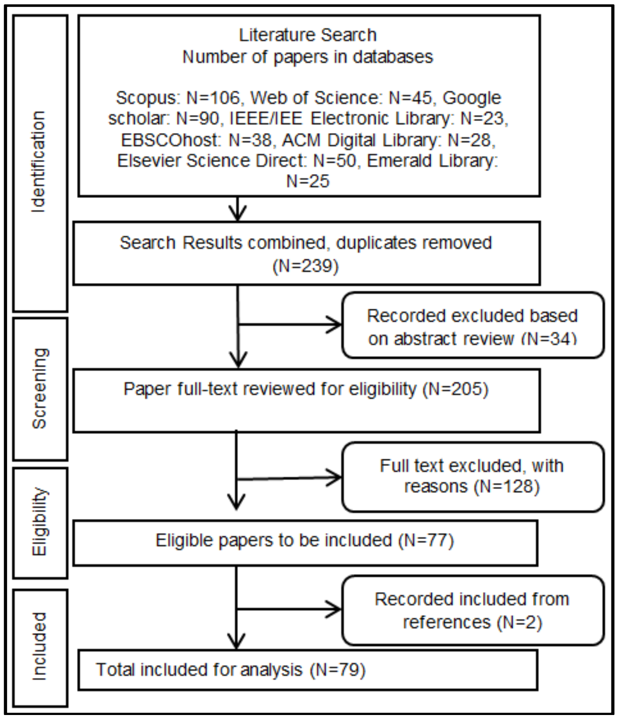

Identification
Screening
Eligibility
Included
Literature Search
Number of papers in databases
Scopus: N=106, Web of Science: N=45, Google scholar: N=90, IEEE/IEE Electronic Library: N=23, EBSCOhost: N=38, ACM Digital Library: N=28, Elsevier Science Direct: N=50, Emerald Library: N=25
Search Results combined, duplicates removed (N=239)
Recorded excluded based on abstract review (N=34)
Paper full-text reviewed for eligibility (N=205)
Full text excluded, with reasons (N=128)
Eligible papers to be included (N=77)
Recorded included from references (N=2)
Total included for analysis (N=79)

Figure 1: Flow diagram regarding the systematic search, inclusion and exclusion of studies in [8].
Source: [8]

Furthermore, instead of using eight databases a in [8], this review only focus on three databases only, which are Web of Science, Scopus and Google Scholar. While the first two databases are containing the top quality papers, the selection of Google Scholar wider the scopes of searching as this database contain almost all the papers published in other indexed and non-indexed databases. Master and PhD theses are excluded from this study. Study by [9] is excluded since this study is specifically based on review on previous ISC studies that not specifically discuss from the context of Malaysian organization.

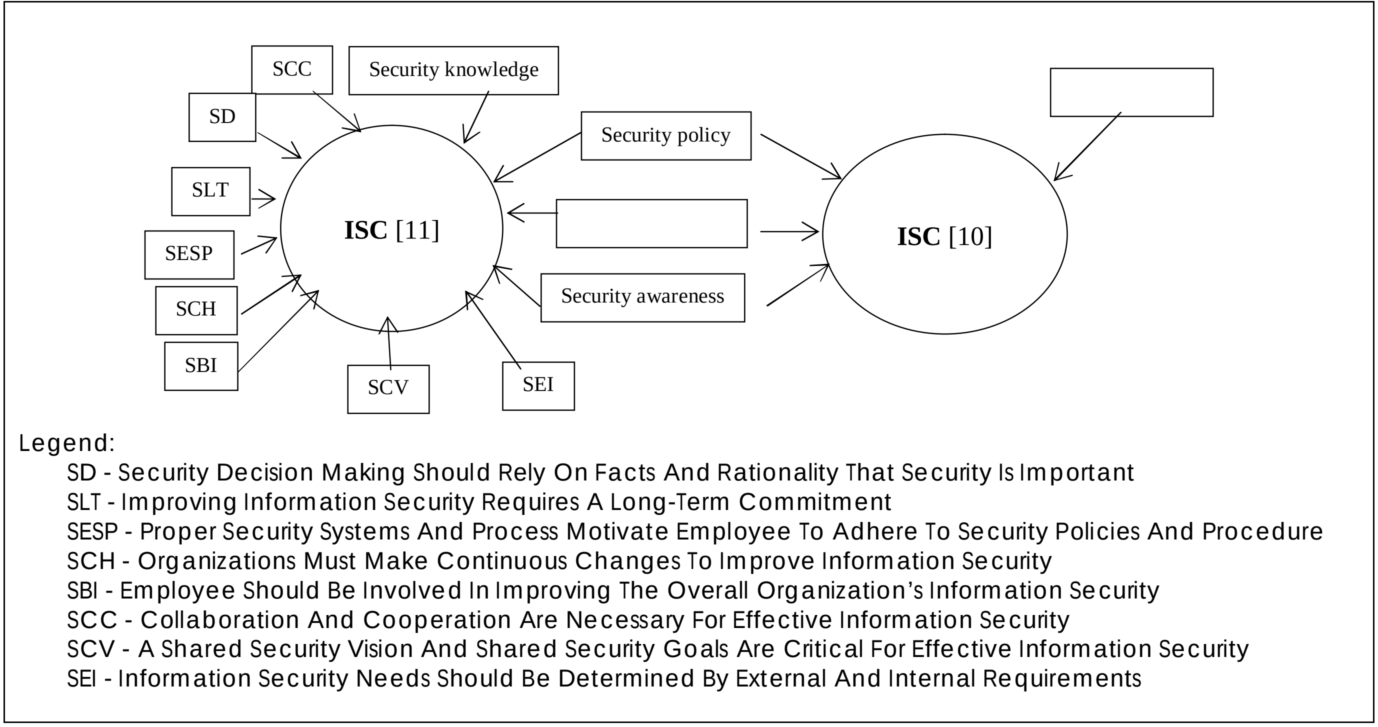
3. FINDINGS

The searching process based on aforementioned technique and criteria has resulted as many as six papers that eligible for further analysis. This is an indication that despite the importance of establishing a positive ISC in an organization, our review found that there are relatively lack of studies have been conducted to develop ISC model for Malaysian organizations. Currently, there are only three validated models have been produced for particular organizations in Malaysia, which is healthcare, library and public organization.

As the main objective of this review is to identify ISC model that could be used as the guidelines to establish ISC in Malaysian organizations, one of the key elements we are analysing on these models is the factors or dimensions. These factors and dimensions are actually representing specific aspects, efforts and measure of ISC that could be used as guidelines to establish ISC in an organization.

Our review found that there are the differences in terms of factors to establish ISC in each types of organization. Interestingly, the differences also found in the ISC models for the same type of organization under study. As shown in Figure 2, in developing ISC models for healthcare organization, [10] found four factors of ISC whereas [11] found twelve factors. Although three factors in [10] which are security policy, security behavior and security awareness are also among the factors in [11], clearly there are two sets of factors involved for the same type of organization as shown in Figure 2. There are some key factors in [11] that did not involved at all in [10] such as top management and change management. Although both studies employed the same methodolgy which is qualitative, we found out that the most relevant reason for this difference is both studies were employed two different concepts in identifying and selecting the factors. However, since security behavior, security awareness and security policy are found in both studies. This suggest that these three factors are important and common for ISC in healthcare organization. This is consistent with [9], [12] that found these three factors are among the key factors of ISC in the organization, particularly in healthcare.

As for public organization and library, the model of ISC are as depicted in Figure 3 and Figure 4 respectively. From the six factors of ISC model for public organization studied by [13]–[16], only one factor of policy and procedures was found to be the same with factors of principles in ISC model for library. This is becase factor principle in ISC model for libarary in [17] was referring to security policy. This means that ISC model for both types of organizations are different even though public library is also one of the organization under Malaysian public organization. Nevertheless, since security policy is the only factor found to be the same, and it was also found in healthcare organization, this suggests that this factor is the must for every organization. This is consistent with [8] that argued ISP is the key factor for any organization in establishing ISC. It is the main artifacts that must be presence in an organization in cultivating ISC [8].



Legend:

SD - Security Decision Making Should Rely On Facts And Rationality That Security Is Important
SLT - Improving Information Security Requires A Long-Term Commitment
SESP - Proper Security Systems And Process Motivate Employee To Adhere To Security Policies And Procedure
SCH - Organizations Must Make Continuous Changes To Improve Information Security
SBI - Employee Should Be Involved In Improving The Overall Organization's Information Security
SCC - Collaboration And Cooperation Are Necessary For Effective Information Security
SCV - A Shared Security Vision And Shared Security Goals Are Critical For Effective Information Security
SEI - Information Security Needs Should Be Determined By External And Internal Requirements

Figure 2: ISC Model for Malaysian Healthcare[10], [11]

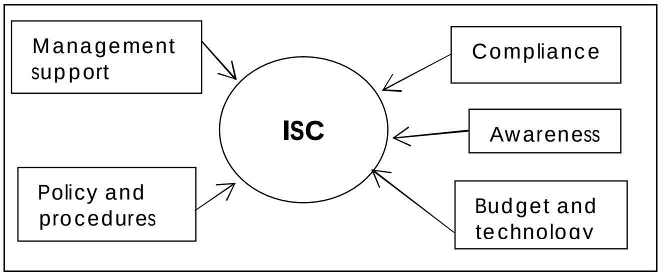


Figure 3: ISC Model for Malaysian Public Organization [13]–[16]

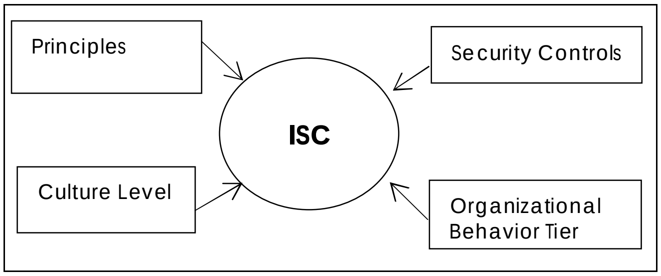


Figure 4: ISC Model for Malaysian Library [17]

4. DISCUSSION

Based on findings above, we found that although ISC is a culture that recommended to be established in the organization, there is still lacks of model could be referred by practitioners in several aspects. First, the model is limited only to three types of organization, which are healthcare, public organization and library only. Since there are many more types of organization such as finance, educational and military in Malaysia, this scenario creates problems for practitioners in establishing ISC in these particular organizations. Furthermore, the breaches also could happen to these organizations; therefore, they also need ISC model to be used as a guideline in improving information security behavior of employees so that they could minimize the security threats.

Secondly, the findings suggest that there is no mutual agreement on the factors of ISC models for each types of organization. To a certain extent, the factors are different even though the models are developed for the same types of Malaysian organization. Since these factors are actually representing the elements, aspects and effort of ISC, the findings suggest that there is lack of common aspects to be used in ISC establishment. Nevertheless, there is one element that always vital in ISC, which is ISP as the findings show that all models have this factor. This also means that ISP is a compulsory in ISC establishment in any Malaysian organization.

Security policy or Information Security Policy (ISP) is defined as a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations [18]. It encompasses established rules that address specific security issues by providing instructions to the employees as to what they should do when they interact with the information and technology resources of their organizations [19]. ISP is one of the vital tools to ensure the secure use of information assets and data in an organizational context [24]. It is the first and foremost requirement for planning, implementing and maintaining information security in an organization. Not having such a high-level policy is regarded as one of the ten most deadly sins of information security management [25].

According to [26], having formal and documented security policies in place is an initial step to shape security culture in an organization. Many studies have considered policies, procedures, guidelines and ethical codes as important elements in cultivating ISC [17], [27]–[34]. [35] empirically found that ISC is more positive if the employees read the ISP. This finding proved the impact and significant role of ISP towards ISC in an organization. It is even considered as the best practice in the field of information security management according to regulations and industry standards (e.g. ISO (International Organization for Standardization)/ IEC (the International Electrotechnical Commission) 27001).

Finally, the findings suggest that despite of the importance of ISC, there is still lack of clear understanding of what is ISC concept and model. As argued in [8], every ISC studies tend to use different concept based on factors and dimension of ISC and this also happened in ISC models in Malaysian context. Although [36] argued that ISC concept is still evolving, a clear and standard concept or model of ISC should be produced so that it could be used as a reference model to all organization even though there might be differences in terms of some aspects.

5. LIMITATIONS AND FUTURE WORKS

Although we believe that we have conducted a thorough searching process to select the papers in this review study, there might be some paper missed out due to the limitation in databases selected. However, as we also included a universal database of Google scholar, this will minimize the chance of missing the articles since this database also publishing articles from most of the other databases.

Apart from that, since this review revealed that there are some issues of inconsistency of ISC dimensions for particular type of organization, more studies need to be conducted to investigate this issue so that a clear ISC model for each type of organization could be produced. Furthermore, there are many more types of organization such as finance, educational and military in Malaysia, more studies should be conducted to find the solid model for these organization.

We also strongly believe that a standard model that applicable for all type of organization should be proposed and validated so that everyone could referring to the same model when talking about ISC.

6. CONCLUSION

This review provides a clear picture on the current status of ISC model for particular type or organizations in Malaysia. Based on systematic search on three major databases, we found that there is a lack of studies has been conducted to develop and validate ISC model for Malaysian organization. Currently, only three types of organizations that have ISC model to be referred, which are healthcare, public library and public organization. However, we have discovered some issues in terms dimensions applicable in the ISC models for these organizations and need further studies.

ACKNOWLEDGEMENT

This research is supported by UMP Post Graduate Research Grant Scheme, PGRS170303. The authors fully acknowledged Universiti Malaysia Pahang (UMP) for the approved fund, which makes this important research viable and effective.

REFERENCES

1. S. Alfawaz, K. Nelson, and K. Mohannak, “Information security culture: A behaviour compliance conceptual framework,” Conf. Res. Pract. Inf. Technol. Ser., vol. 105, pp. 47–55, 2010.
2. P. A. H. Williams, “What does security culture look like for small organizations?,” in Australian Information Security Management Conference, 2009, no. December, pp. 48–54.
3. A. Alhogail, “Design and validation of information security culture framework,” Comput. Human Behav., vol. 49, no. August 2015, pp. 567–575, 2015. https://doi.org/10.1016/j.chb.2015.03.054
4. J. Van Niekerk and R. Von Solms, “Information security culture: A management perspective,” Comput. Secur., vol. 29, no. 4, pp. 476–486, 2010.
5. J. S. Lim, S. Chang, S. B. Maynard, and A. Ahmad, “Exploring the Relationship between Organizational Culture and Information Security Culture,” in 7th Australian Information Security Management Conference, 2009, no. December, pp. 88–97.
6. A. Greig, K. Renaud, and S. Flowerday, “An Ethnographic Study to Assess the Enactment of Information Security Culture in a Retail Store,” pp. 61–66, 2015.
7. A. Mahfuth, S. Yussof, A. A. Baker, and N. Ali, “A systematic literature review: Information security culture,” in 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), 2017, pp. 1–6. https://doi.org/10.1109/ICRIIS.2017.8002442
8. A. Nasir, R. A. Arshah, M. R. A. Hamid, and S. Fahmy, “An analysis on the dimensions of information security culture concept: A review,” J. Inf. Secur. Appl., vol. 44, pp. 12–22, 2019.
9. 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, no. ICIBSoS, pp. 1007–1012, 2012.
10. N. H. Hassan and Z. Ismail, “Information Security Culture in Healthcare Informatics: A Preliminary

Investigation," J. Theor. Appl. Inf. Technol., vol. 88, no. 2, pp. 202–209, 2016.

11. N. H. Hassan, N. Maarop, Z. Ismail, and W. Z. A. Advanced, "Information Security Culture in Health Informatics Environment : A Qualitative Approach," 2017.
12. N.H. Hassan, Z. Ismail, and N. Maarop, "Information Security Culture: A Systematic Literature Review," no. 205, pp. 456–463, 2015.
13. M. NoormanMasrek, Q. Nazrin Harun, and M. KhairulnizanZaini, "Information Security Culture for Malaysian Public Organization: A Conceptual Framework," in Proceedings of INTCESS 2017 4th International Conference on Education and Social Sciences, 2017, pp. 156–166.
14. M. N. Masrek, Q. N. Harun, and M. K. Zaini, "The Development of an Information Security Culture Scale For The Development Of An Information Security Culture Scale For The," Int. J. Mech. Eng. Technol., vol. 9, no. July, pp. 1255–1267, 2018.
15. M. N. Masrek, "Assessing Information Security Culture : The Case of Malaysia Public Organization," Proc. 2017 4th Int. Conf. Inf. Tech., Comput. Electr. Eng. (ICITACEE), Oct 18-19, 2017, Semarang, Indones. Assess., p. 5386, 2017. https://doi.org/10.1109/ICITACEE.2017.8257663
16. M. N. Masrek, "Assessing the Information Security Culture in a Government Context : The Case of a Developing Country," vol. 9, no. 8, pp. 96–112, 2018.
17. [17] M. S. Shahibi, R. M. R. S. K. W. Fakeh, and W. A. K. W. D. J. Ali, "Determining Factors Influencing Information Security Culture Among ICT Librarians," vol. 37, no. 1, pp. 132–140, 2012.
18. B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," Br. J. Anaesth., vol. 106, no. 2, pp. 199–201, 2010.
19. M. E. Whitman, "Security Policy: From Design to Maintenance," Adv. Manag. Inf. Syst., vol. 11, pp. 123–151, 2008.
20. S. R. Boss and L. J. Kirsch, "The last line of defense: Motivating employees to follow corporate security guidelines," Icis, pp. 1–18, 2007.
21. J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Inf. Syst. Res., vol. 20, no. 1, pp. 79–98, 2009.
22. T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," Eur. J. Inf. Syst., vol. 18, no. 2, pp. 106–125, 2009.
23. T. R. Peltier, Information security policies and procedures : a practitioner's reference. Auerbach Publications, 2004. https://doi.org/10.1201/9780203488737
24. L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," Comput. Secur., vol. 39, pp. 447–459, 2013.
25. B. von Solms and R. von Solms, "The 10 deadly sins of information security management," Comput. Secur., vol. 23, no. 5, pp. 371–376, 2004.
26. Y.A.N. Chen, K. R. A. M. Ramamurthy, and K. Wen, "Impacts of Comprehensive Information Security Programs on Information Security Culture," J. Comput. Inf. Syst., vol. 55, no. 3, pp. 11–19, 2015.
27. R. Von Solms and B. Von Solms, "From policies to culture," Comput. Secur., vol. 23, no. 4, pp. 275–279, 2004. https://doi.org/10.1016/j.cose.2004.01.013
28. A. Da Veiga and N. Martins, "Information security culture and information protection culture: A validated assessment instrument," Comput. Law Secur. Rev., vol. 31, no. 2, pp. 243–256, 2015.
29. M. A. Alnatheer, "Understanding and Measuring Information Security Culture in Developing Countries : Case of Saudi Arabia," Queensland University of Technology, 2012.
30. M. A. Alnatheer, "A Conceptual Model to Understand Information Security Culture," Int. J. Soc. Sci. Humanit., vol. 4, no. 2, pp. 104–107, 2014.
31. 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.
32. S. Dojkovski, S. Lichtenstein, and M. J. Warren, "Enabling information security culture: influences and challenges for Australian SMEs," in 21st Australasian Conference on Information Systems, 2010, p. 61.
33. M. A. Alnatheer, "Information Security Culture Critical Success Factors," in 2015 12th International Conference on Information Technology - New Generations, 2015, pp. 731–735.
34. A. Martins and J. Eloff, "Information Security Culture," Secur. Inf. Soc., vol. 86, no. April, pp. 203–214, 2002. https://doi.org/10.1007/978-0-387-35586-3_16
35. A. Da Veiga, "The Influence of Information Security Policies on Information Security Culture : Illustrated through a Case Study," no. Haisa, pp. 22–33, 2015.
36. E. Kolkowska, "Security Subcultures in an Organization - Exploring Value Conflicts," 2011.
37. Sami Haji , Qing Tan, and Rebeca Soler Costa. A Hybrid Model for Information Security Risk Assessment. Sami Haji et al., International Journal of Advanced Trends in Computer Science and Engineering, 8(1.1), 2019, 100 – 106. Volume 8, No.1.1, 2019 https://doi.org/10.30534/ijatcse/2019/1981.12019