International Journal of Synergy in Engineering and Technology
IJSET

How to Cultivate Cyber Security Culture? The Evidences from Literature

Akhyari Nasir[1], Syahrul Fahmy[2], Wan Roslina Othman[1], Noor Suhana Sulaiman[1], Nooraida Samsudin[1], Azham Ahmad[1] and M R A Hamid[3]

[1] Faculty of Computer, Media & Technology Management, UC TATI, Terengganu, MALAYSIA
[2] Big Data Institute, UC TATI, Terengganu, MALAYSIA
[3] Faculty of Industrial Management, Universiti Malaysia Pahang, Pahang, MALAYSIA

Corresponding author e-mail: akhyari@uctati.edu.my

KEYWORDS

Cyber Security Culture
Information Security Culture

ABSTRACT

Cyber Security Culture (CSC) is a culture that could produce a secure cyber space and could improve the quality of cyber world engagement. Despite many benefits that could be offered by CSC, there is a lack of models and guidelines on how to cultivate this culture. This paper discusses the concept of CSC model in terms of elements that form the model to suggest how CSC could be cultivated. Information Security Culture (ISC) model developed by [1] is used as a framework in discussing the concept of CSC. A literature search also is conducted to find and analyses the most suitable elements for CSC. A new model of CSC was proposed as a result of this study. The findings could provide better understanding of CSC and could be used as baseline to conduct more research on CSC.

1.0 Introduction

Many experts and scholars proposed Cyber Security Culture (CSC) as a culture that could be fostered in order to improve information security of a nation. In terms of definition, CSC is similar to Information Security Culture (ISC). According to [2], practitioners recommended ISC to be cultivated in guiding the security behaviour in an organization. However, CSC is having a wider scope in terms of coverage and component. It is because the nature of the information security and cyber security are different [3]. While ISC is applicable to an organization, CSC is applicable to a nation or country [4].

According to [5], CSC refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cyber security and how they manifest in people's behaviour with information technologies. This definition implies that CSC is a culture that could be cultivated to influence security behaviour of the people that finally will ensure the security of cyber space of a nation.

Received 20 October 2022; received in revised form 15 December 2022; accepted 31 January 2023.

Despite the benefits that have been proposed by many experts and scholars, there is still lack of clear indication of the elements that form the CSC. This scenario would give a mix understanding on CSC and would lead to mislead when referring to the CSC concept. The elements of CSC are important since they could be used to understand CSC and could be used to plan and cultivate this desired culture. Rayne Reid & Van Niekerk (2014a) has produced a comprehensive study to justify the CSC concept based on components. However, more study should be conducted to get more finding on this particular area. This paper discusses this issue and provides the elements and strategies to cultivate a promising and successful CSC. The next section will review the related literature followed by the methodology applied for this study. Then the following section discusses the result and discussion of the study. Finally, the conclusion will be presented at the end of the section.

2.0 Literature Review

In literature, there is a lack of reference model that could be used to model CSC. However, most of the researchers define CSC as the same concept with ISC but in wider scope. While ISC applicable to an organization, CSC scope is applicable to a nation or country [4], [6]. Within these researchers, most of them used ISC model based on [1] to discuss CSC. This model was derives from and expands Schein's organizational culture model [4].

Figure 1 shows adaptation of levels in Organizational Culture (OC) of [7] for ISC Model. OC consists of three levels, which are artefacts, espoused values and shared tacit. These three levels of OC were adapted by [1] to conceptualize ISC and added one more level, which is Information Security Knowledge (ISK) as illustrated in Figure 1. They believed that this new level is important to differentiate OC from ISC. These three levels are for a normal OC and ISK level underpins and supports all three the "normal" levels of corporate culture to form an effective ISC in the organization. According to [1], if an organization is trying to foster a sub-culture of information security, all activities would have to be performed in a way that is consistent with good information security practice. Therefore, having adequate knowledge regarding information security is a prerequisite to performing any normal activity in a secure manner.

The ISC conceptual model by [1] is focussing on the functions and the importance of information security knowledge towards three levels of OC in forming the stable ISC. According to Niekerk and Solms (2006), at the Artefacts level, the sufficient knowledge ensure the activities are performed safely manner. According to [8], the artefacts of CSC could be involved national policy, laws and other recommended best practices.

At the Espoused Value level, the knowledge determines what to include in a policy in order to adequately address the organization's information security needs. According to [8], this level strongly relates to the artefacts level and suggested that "the espoused values would likely be issued by governmental, national or international agencies and would then manifest as a national cyber security culture."

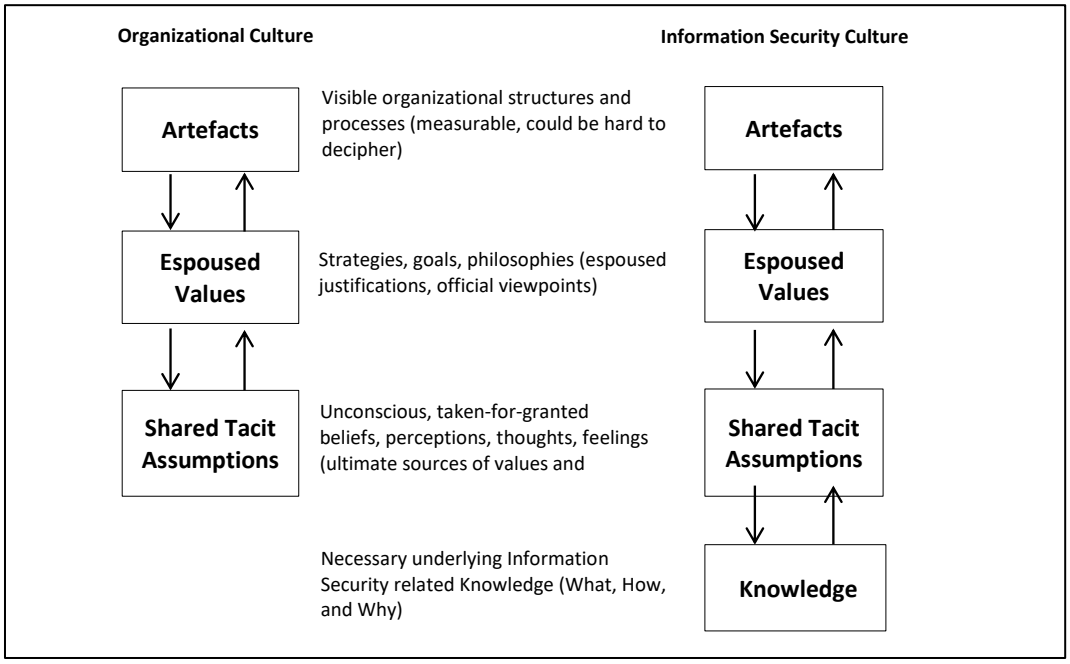

Figure 1: Adaptation of levels in Organizational Culture for ISC Model
Source: [1]

As for Shared Tacit Assumptions, this level consists of the beliefs and values of the employees. If such a belief should conflict with one of the espoused values, with adequate knowledge, knowing why a specific control is needed, might play a vital role in ensuring compliance [9]. As for ISC this level of corporate culture directly influences the behaviour of employees that can be observed at the artefact level [4]. However in CSC, according to [4] the component of this level will be more difficult to observe.

The fourth level in ISC model is Knowledge. This knowledge is required to respond and react to information security matters. According to [8], "this relates to awareness of the requisite security knowledge needed to fulfil the user's security roles while they are completing a task." The ISC conceptual model by [1] suggests that each of the underlying cultural levels will contribute towards the overall strength and stability of such a culture.

3.0 Methodology

In this study, the four levels in Information Security Culture (ISC) model by [1] is used as a framework of CSC model. Based on the definition, each level will be mapped and assigned with suitable elements. These elements are taken from the literature. Finally, a new concept of CSC was proposed.

4.0 Results and Discussion

Table 1 shows the results of mapping and assigning of CSC elements into the corresponding level. The last column shows the studies where the elements were taken from. As shown in the table, most of the elements and components come from study by [4]. This means that their study is the most comprehensive study on this particular area.

Table 1: Levels and Elements of CSC

Level	Elements	Authors
Artefacts	National Information Security Policy, Right and Laws	[6], [8]
Espouse Value	Enforcement	[10], [11]
Shared Assumptions	Set of accepted norms and behaviour of security that government try to foster	[12][13], [4], [6]
Knowledge	SETA/Education	[6], [8]
	Campaign	[6]

As mentioned in Literature Review section, most of the scholars agreed that CSC is similar to ISC but with wider scope. ISC is for an organization while CSC is applicable to a nation or country. Figure 2 shows the adaption of four levels of ICS model by [1] to be used as a framework to proposed new CSC model in this study. The following subsections discuss the justification of CSC levels and its elements of the CSC model.

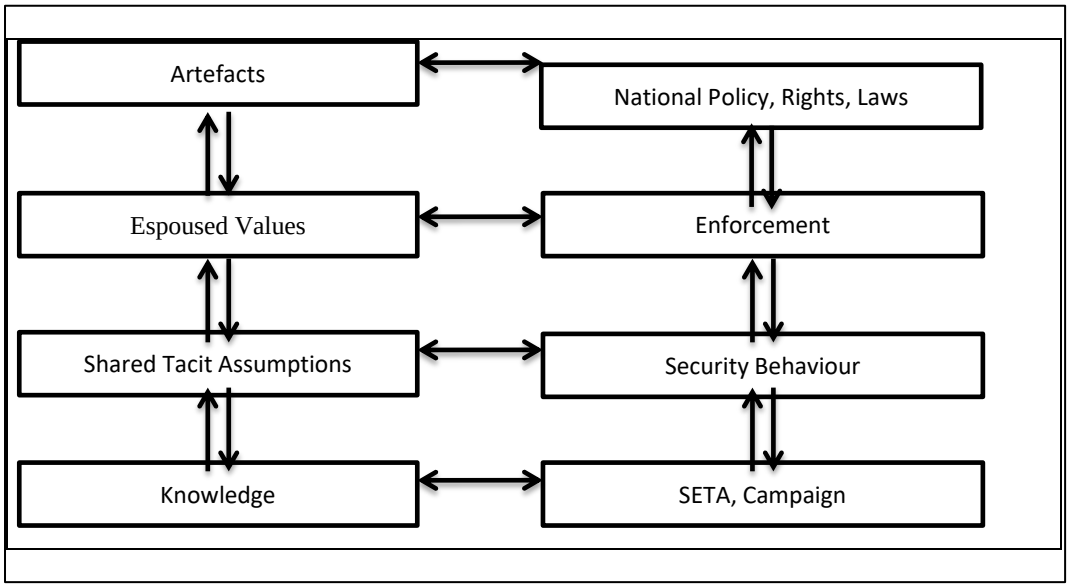

Figure 2: The adaptation of ISC framework to propose CSC framework

4.1 Level 1 – Artefacts

According to [14], "artefacts are what you can observe, see, hear, and feel, in an organization". In CSC, it is something that represents national policy, rights and laws of cyber security. The existence of these elements symbolize that a country has clear objectives and practicing a culture of cyber security. For example, Malaysian government has a National Cyber Security Policy (NCSP). Among others, the vision of this policy clearly said that "Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well-being and wealth creation" [15].

Malaysia also has its own laws and rights related to cyber security such as Computer Crimes Act 1997, Communications and Multimedia Act 1998, Penal Code, Copyright Act 1987 and Personal Data Protection Act 201. All these elements of artefacts clearly indicate that Malaysia has an established CSC artefact that could influence the Malaysian towards CSC.

4.2 Level 2 - Espoused Value

According to [8], artefacts and espoused Values are strongly related to each other. Values taken directly from the artefacts are espoused in the culture through the strategy. Here the enforcement is important to make sure that all the proposed values in the NCSP, Rights and Laws are followed and complied. This enforcement is a strategy taken to make sure all the cyber security artefacts are followed and complied.

Most of the governments are lacking this element. Even if there are the enforcements implemented, but there are not quite clear to the public. There are some laws have been established but they are still not holistic in terms of the contents, communications and enforcements.

The implementation of CSC enforcement is to ensure all the laws, policies and rights are followed. The enforcement's contexts are based on these artefacts. All the content in those artefacts will be enforce through this level of espoused values. In organizational context, enforcement is easier to be implemented such as by performing security audits and monitoring to ensure the information security policy is followed by the employees. However, in national context, it is a harder effort.

4.3 Level 3 - Shared Tacit Assumptions

The enforcement of CSC values would make and shape the security behaviour of the citizen. The behaviour that are desired in CSC are including the knowledge, skills, attitude and awareness in dealing and communicating in cyber space. These behaviours not only assisting people to use, adopt and adapt with cyber world facilities, it would also protect people from various threats such as phishing scams and cyberbullying.

The best way to protect people against cyber security threats or cybercrime is to provide them with the appropriate awareness and knowledge [16]. It is includes providing them with the information on security threats and security measures associated to the threats. According to [17], government could uses social media accounts to help provide people with knowledge and tips about current information security threats. In this way, they are always ready and updated with the latest information and awareness of cybersecurity.

4.4 Level 4 – Knowledge

The desired security behaviour of the people is not claimed without training and educating them. Here where the Security Education, Training and Awareness (SETA) and other security campaigns play the roles. This is how the knowledge and awareness of CSC to the citizens could be distributed in order for them to get the correct and meaningful information and knowledge These elements located in level four of ISC model by [1].

SETA and security campaign that are planned and implemented are based on the elements in artefacts, which are the NP, Rights and Laws. Every policy, laws and requirements of cyber security from the government will be communicate, educate, train and updated through these level of CSC. According to [18], the implementation and designing the SETA programs is essential to improve cyber security. As a result, it will produce behaviour of cyber security that consistent with the ambition by the government until it will become a culture that called CSC.

5.0 Limitations and future works

Although this study proposed the elements that form the concept of CSC, it has some weaknesses and limitations. Obviously, the study did not use a comprehensive and systematic literature review in findings the elements that could fits the four levels of the framework. There might be another element that were missing in this study. However, since this study was using a comprehensive framework, all the CSC elements that would be found are only applicable if they fit the definition of the particular levels in the framework. Nevertheless, a more comprehensive

study should be conducted to address this issue so that a CSC model with a set of comprehensive elements could be proposed.

6.0 Conclusion

Cyber Security Culture (CSC) is a culture that could be cultivated using the same approach of Information Security Culture (ISC). Using four levels of ISC framework, a new CSC model was proposed with a set of elements that form the culture. While all the four of ISC are applicable to CSC, CSC has a wider scope in terms of the elements. These elements are the strategies and factors that could be used to cultivate CSC.

Acknowledgments

This research is supported by UC TATI Short-Term Grant (STG) GPJP 1/2020 I-GOT 9001-2012. The authors fully acknowledged University College TATI (UC TATI) for the approved fund, which makes this important research viable and effective.

References

[1] J. Van Niekerk and R. Von Solms, "Understanding Information Security Culture: A Conceptual Framework," in Proceedings of ISSA 2006, 2006, pp. 1–10.
[2] A. Nasir, M. Rashid, and A. Hamid, "Conceptualizing and Validating Information Security Culture as a Multidimensional Second-Order Formative Construct," in The Thirteenth International Multi-Conference on Computing in the Global Information Technology, 2018, pp. 1–8.
[3] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: Current practices and future needs," Comput. Secur., vol. 109, 2021, doi: 10.1016/j.cose.2021.102387
[4] R. Reid and J. Van Niekerk, "From information security to cyber security cultures," 2014 Inf. Secur. South Africa - Proc. ISSA 2014 Conf., no. January, 2014, doi: 10.1109/ISSA.2014.6950492
[5] ENISA, "Cyber Security Culture in Orginisations," Eur. Union Agency Netw. Inf. Secur., 2017.
[6] R. Reid and J. Van Niekerk, "Towards an education campaign for fostering a societal, cyber security culture," 2014.
[7] E. H. Schein, Organizational culture and leadership, vol. 7, no. 2. 1992.
[8] R. Reid and J. Van Niekerk, "From Information Security to Cyber Security Cultures Organizations to Societies," 2014, doi: 978-1-4799-3383-9.
[9] T. Schlienger and S. Teufel, "Information security culture: from analysis to change," South African Comput. J., vol. 31, pp. 46–52, 2003.
[10] K. Bounas, A. Georgiadou, M. Kontoulis, S. Mouzakitis, and D. Askounis, "Towards a cybersecurity culture tool through a holistic, multi-dimensional assessment framework," 2020.
[11] CyberSecurity Malaysia, "Cyber security trends & strategy for business (digital ?)," 2015.
[12] N. Gcaza, R. Von Solms, and J. Van Vuuren, "An ontology for a national cyber-security culture environment," 2015.
[13] J. J. van V. Noluxolo Gcaza, Rossouw von Solms, Marthie M Grobler, "A general morphological analysis : Delineating a cyber security culture," Inf. Comput. Secur., 2017.
[14] E. H. Schein, The Corporate Culture Survival Guide. Jossey-Bass Inc., 1999.
[15] N.C.S.A. (NACSA), "The National Cyber Security Policy," 2021. https://www.nacsa.gov.my/ncsp.php
[16] M. Martens, R. De Wolf, and L. De Marez, "Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general," Comput. Human Behav., vol. 92, no. October 2018, pp. 139–150, 2019, doi: 10.1016/j.chb.2018.11.002

[17] Z. Tang, A. S. Miller, Z. Zhou, and M. Warkentin, "Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations," Gov. Inf. Q., vol. 38, no. 2, 2021, doi: 10.1016/j.giq.2021.101572

[18] M. I. Alghamdi, "Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia," Mater. Today Proc., no. xxxx, 2021, doi: 10.1016/j.matpr.2021.04.093.