INFORMATION SECURITY CULTURE: A SYSTEMATIC LITERATURE REVIEW

Noor Hafizah Hassan[1], Zuraini Ismail[2], and Nurazean Maarop[3]

[1]Universiti Teknologi Malaysia, Malaysia, nhafizah95@live.utm.my
[2]UniversitiTeknologi Malaysia, Malaysia, zurainiismail.kl@utm.my
[3]Universiti Teknologi Malaysia, Malaysia, nurazean.kl@utm.my

ABSTRACT. Information security culture becomes an enabler towards minimising the protection of security risk and incidents. This research will systematically identify and analyse published research exploring factors influencing information security culture. A systematic literature review is conducted throughout this process. 40 papers were used in our synthesis of evidence with nine compatibility factors has been found to influence information security culture in organisation setting. One thousand two hundred and four studies were identified as 40 fulfilled the inclusion criteria. Of these, most (13%) were assessed being high quality, and three were rated very poor. Nine common factors were identified which are cultural differences, security awareness, security behaviour, top management commitment, trust, information sharing, security knowledge, security policy, and belief. The most common factors found was security behaviour that highly influences information security culture from analysis conducted. The result of this study also shows the gap that there is lack of studies conducted in healthcare informatics environments setting. Findings are useful in developing theoretical model that shows factors influencing information security culture in healthcare informatics environment.

Keywords: security culture, organizational culture, systematic literature review

INTRODUCTION

Information security is defined as the activity to protect information from a wide range of threats in order to ensure business continuity, minimise business damage, and maximise return on investments and business opportunities (Hagen, Albrechtsten, & Hovden, 2008). In healthcare informatics, a growing concern on security in healthcare are increasing (Appari & Johnson, 2010). Despite the potential for quality improvement, the concerns about the privacy and security of patient data are viewed as a barrier to the healthcare informatics usage (Boonstra & Broekhuis, 2010; Granlien & Hertzum, 2012). Besides, it has been reported that various threat attacks have been found in hospital information systems (HIS) (Samy, Ahmad, & Ismail, 2010). This trend, along with the advances in health informatics is expanding the demand to build an effective information security protection for healthcare organisation. The innovation which aims towards enhancing quality of life, diagnostic and treatment options, as well as the efficiency and cost effectiveness of the healthcare system lead to the issues on the information security (Omachonu & Einspruch, 2010). One of the area that has been addressed by Gaunt (2000) are by cultivating information security culture in medical informatics. In

2000, Van Niekerk and Von Solms (2010) investigated how corporate culture influence the effectiveness of information security culture through knowledge.

Vroom and Solms (2004) suggest that organisational role is important to have an effective information security culture. Thus, one important aspect is to understand the underlying factors that make information security culture to contribute towards successful information security practise. Our research aims to identify key factors influencing information security culture in health informatics. This research applies a systematic literature review (SLR) in assessing the existing information security cultures' literature. The key contribution of this paper is the findings from the SLR of empirical studies of information security culture in organisations from 2000-2014. This may help to inform organisations wanting to implement information security policy to a better information security management system. Findings from the SLR are presented with gaps in the existing body of knowledge are highlighted. These suggest key area of focus that should be highlighted in information security culture research. In section 2, this paper describes the method adopted in SLR. Section 3 provides reports from the SLR results based on the synthesis of evidence. The next section provides a discussion of key findings, implications, limitation, and future works. The last section gives an overall conclusion from the SLR conducted.

THE REVIEW METHOD

SLR also referred as secondary study is defined as the process of identifying, evaluating, and interpreting related research area pertaining to the research question and area that has been identified (Kitchenham, 2004). This study followed the original guideline by Kitchenham et al.(2009) as presented in the following section.

Research Question

Population, Intervention, Comparison, Outcomes, and Context (PICOC) structure of questions are shown in Table 1. The primary focus in this study was to understand and identify the factors that influence the effectiveness of information security culture practice in any organisation. In order to identify to what extent the information security culture study has been conducted, this work investigates to answer the following primary research questions:

Table 1. Summary of PICOC

Population	Any organisation
Intervention	Information Security Culture
Comparison	None
Outcomes	Information Security Culture
Context	Review (s) of any empirical studies of information security culture within the domain of any applied case study setting in any organisation. No restriction on the type of study applied

Primary question: What are the evidences of any information security culture studies conducted in any environment settings that investigated information security culture effectiveness align with information security policy?The study of SLR also aimed to answer the following secondary sub question:Sub question 1:What evidence is there regarding factors that affect information security culture, and which are the most effective factors?Sub question 2: How was the information security culture study has been conducted and being implemented in previous studies? Sub question 3: Is there any information security culture studies conducted in healthcare settings?

Study Selection and Research Resources

Based on the identified research questions, a study selection criterion must be identified to support the direct evidence to reduced likelihood of bias. Upon the completion of the primary research phase, this research follow the process suggested by Salleh, Mendes, and Grundy (2011) that has refine their search in secondary search phase. The references on the selected papers from primary search phase are thoroughly reviewed. If the paper meets the criteria of selection, then the paper will be included for synthesis.

The primary search process involved the use of nine online databases: ACM Digital library, Emerald, EBSCOhost, IEEEXplore, Sage Full Text Collections, ScienceDirect, SpringerLink, Wiley, and Taylor and Francis.Depending on the search services offered by the relevant search engines, the following search terms as follows: (Information security culture OR security culture OR organizational culture OR culture), AND (experiment OR measurement OR evaluation OR assessment) AND (information security).

Inclusion and Exclusion Criteria

The main inclusion criterion for this study is to include the security culture practice in any organisation that has been conducted. Peer reviewed articles published from 2000- 2014 are taken into consideration for the inclusion in search criteria. The detail inclusion criteria included are:

- Studies that investigate the effectiveness of information security culture.
- Studies that investigate the concept of organisational culture towards information security.
- Studies that measure the effectiveness of security culture in any organisation.

Meanwhile, the articles that are excluded from our research criteria are:

- Papers that are claiming another author that has no supporting evidence.
- Papers that only describe the concept of security culture.
- Papers that are not written in English.

Data Extraction and Study Quality Assessment

In ensuring that the data extraction process meets the quality criteria, hence study checklists need to be prepared accordingly (Kitchenham et al., 2009). Following that, this study reuse the quality criteria checklist from Salleh et al.(2011) has been adopted for SLR. Study quality checklists as shown in Table 2 are the items checklist for the study identified. Our study checklist uses three scale which are coded and given a score which are; Yes=1; Partially = 0.5; No= 0. From the item checklist, each paper will be given a summing on each of the items. Possible scores range from 0.5 to 5 is the highest score.

Table 2. Item Study Checklist

Item	Answer
1. Was the article referred?	Yes/No
2. Was aim of the study is clearly stated?	Yes/No/Partially
3. Were the data collection were carried out well?	Yes/No/Partially
4. Were the study participants were described?	Yes/No/Partially
5. How generalisable are the findings of this study to the target population with respect to the size and representativeness of sample.	Yes/No/Partially

RESULTS

This paper will show the results of the finding from the systematic literature review that has been conducted. Figure 2 shows the summary of the stages of study selection in this SLR guidelines according to Kitchenham (2004). The first iteration involved searching keywords as in Section 2.2 on nine scientific databases. As a result, 1204 primary studies were identified. Two iteration processes have been involved as first iteration involved primary search that produce 53 final primary studies. As in the second iteration, the references contained in the papers are identified in first iteration are examined. The second iteration produces four related identified papers. Each of the articles was filtered according to inclusion and exclusion criteria identified earlier before being accepted by synthesis of evidence. After reading on titles and abstracts, and found that it is insufficient to identify related paper, thus the full articles will be used. It shows that the calculation has been taken before the total number of 187 papers identified after screening the title of the articles.

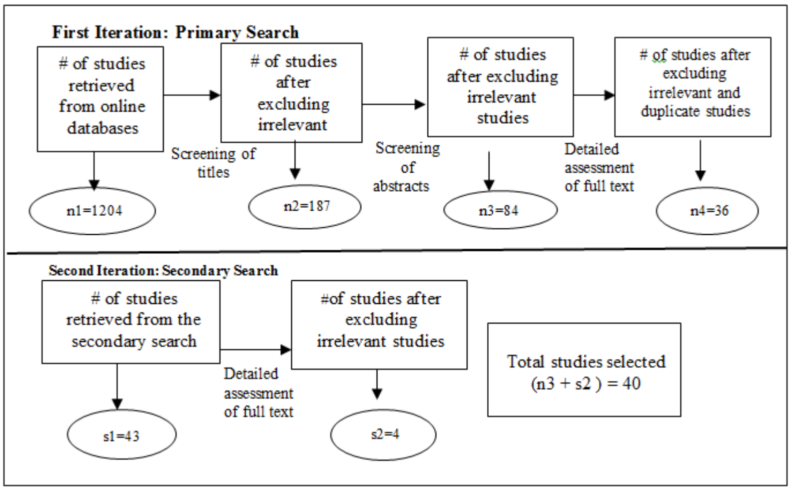
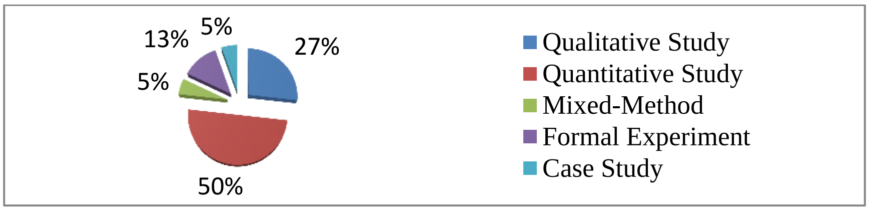

First Iteration: Primary Search
# of studies retrieved from online databases
# of studies after excluding irrelevant
# of studies after excluding irrelevant studies
# of studies after excluding irrelevant and duplicate studies
Screening of titles
Screening of abstracts
Detailed assessment of full text
n1=1204
n2=187
n3=84
n4=36
Second Iteration: Secondary Search
# of studies retrieved from the secondary search
#of studies after excluding irrelevant studies
Detailed assessment of full text
s1=43
s2=4
Total studies selected (n3 + s2) = 40

Figure 1. Stage Selection Process in SLR

An analysis of the type of studies is presented in Fig. 2 which is based on the suggested research types. Quantitative study shows the most chosen research approach in 50% percentage from the total of study. Mixed-method is the least popular approach used in this study that comprises 5% percentage.

Figure 2. Study by Research Approach



Quality Factors

The evaluation of SLR based on quality score as shown in quality checklist in Table 3. Table 1 shows the quality scores for all primary studies. Most of the studies conducted are in good quality criteria. 15 studies (35%), and 5 (12%) were deemed good and very good quality respectively. Three studies are in very poor quality as it did not provide a detailed result and methodology conducted in their study. This study was removed in the analysis phase. Thus in the end, only 40 studies were included for the purpose of analysis of evidence.

Table 3. Result of Quality Checklist

Quality Scale	**Very Poor (>=1)**	**Poor (>=2)**	**Fair (>=3)**	**Good (>=4)**	**Very Good (=5)**	**Total**
Number of Studies	3	10	7	15	5	40
Percentage (%)	7%	24%	18%	38%	13%	100

DISCUSSIONS

In this section, we discuss our result based on the research question developed. We present the synthesis of evidence of SLR conducted.

What evidence is there regarding factors that affect information security culture and which are the most effective factors?

From the SLR studies, 40 information security culture studies conducted in banking, finance, information technology, advertising, marketing, education, engineering, and healthcare environments by professionals on the area of settings have been identified. The SLR ultimate goal was to understand how information security culture affects employee in performing information security practice. From SLR, nine factors identified which are security behaviour, security awareness, top management commitment, cultural differences, trust, information sharing, security knowledge, security policy, and belief. Table 4 demonstrated the result from SLR studies conducted representing the nine factors.

Table 4. Factors Influencing Information Security Culture

Key Factors	**Authors**
Security Behaviour	Zakaria, 2006 ; Ngo, Zhou, Chonka, & Singh, 2009; Alfawaz, Karen, & Mohannak, 2010; Brady, 2011; A. Da Veiga & Eloff, 2010; Shahibi, Rashid, Fakeh, Dollah, & Ali, 2012; Guo, 2013; AlHogail, 2015
Security Awareness	Al-Mayahi & Mansoor, 2013; Donahue, 2011; Gebrasilase & Lessa, 2011; Kraemer, Carayon, & Clem, 2009; Shaaban & Conrad, 2013; Adéle Veiga & Martins, 2015; Woodhouse, 2007
Top Management	D'Arcy & Greene, 2014; Donahue, 2011; Gebrasilase & Lessa, 2011; Hu, Dinev, Hart, & Cooke, 2012; Knapp & Marshall, 2006; Ngo et al., 2009
Cultural Differences	Ngo, Zhou, Chonka, & Singh, 2009; Sabbagh & Kowalski, 2012; Mansouri-Rad, Mahmood, Thompson, & Putnam, 2013; Ifinedo, 2014
Trust	Williams, 2008
Information Sharing	Ghernouti-Hélie, Tashi, & Simms, 2010
Security Knowledge	Zakaria, 2006; Van Niekerk & Von Solms, 2010
Security Policy	Donahue, 2011; N. Martins & Veiga, 2010; Ngo et al., 2009; Shaaban & Conrad, 2013; Hedstrom & Karin, 2014; Lopes & Pedro, 2014; D'Arcy & Greene, 2014
Belief	Ramachandran, 2008; Shahibi et al., 2012; Ashenden & Sasse, 2013; Merhi, 2014

How was the information security culture study has been conducted and being implemented in previous studies?

In a study by Okere et al. (2012), they summarised related studies conducted in information security culture. From their study, it shows that there is no study that applies mix-method research design. Additionally, from this SLR, as inclusion and exclusion criteria is expanded, this research found out that 5% studies employed mixed-method approaches are chosen in the research conducted. In good quality criteria paper, three papers employ quantitative study followed by qualitative studies; the interviews. Only one study adopted exploratory research design (Alnatheer, Chan, & Nelson, 2012) as their research method design.

Is there any information security culture studies conducted in healthcare settings?

Based on the SLR conducted, only one information security culture studies has been conducted in healthcare settings in a hospital in Ethiopia. In this study, they adopted questionnaire from Adele (2002) as they found that security awareness is the most significant factors influence the information security culture in healthcare informatics. Additionally, Williams (2009) has highlighted that trustful culture is the important factors in cultivating in medical information security culture towards the facets of information security governance.

CONCLUSION

This paper described an SLR targeted at empirical studies of information security culture. A total of 40 primary studies were selected and analysed in this SLR that resulted in nine compatibility factors influencing effectiveness of information security culture were identified. Security awareness, cultural differences, security behaviour, and top management commitment were the four factors investigated the most in information security culture studies. Besides that, information sharing, security policy, security knowledge, belief and trust are the least significant factors found in information security culture research. A cultural difference among employee also contributes significant factors as the result collected from individualism and collectivism culture in different countries. The results from this SLR will be used to design conceptual model that represent factors influencing information security culture in health informatics.

REFERENCES

Alfawaz, S., Karen, N., & Mohannak, K. (2010). Information security culture : A Behaviour Compliance Conceptual Framework. *Proc. of Australasian Info Security Conf* , 47–55.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*(2015), 567–575.

Al-Mayahi, I., & Mansoor, S. P. (2013). Information security culture assessment: Case study. In *2013 IEEE Third Int. Conference on Information Science and Technology (ICIST),* 789–792. IEEE.

Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding And Measuring Information Security Culture. In *Pacific Asia Conference on Information Systems (PACIS) 2012* (p. 144).

Appari, A., & Johnson, M. E. (2010). Information Security and Privacy in Healthcare : Current State of Research. *International Journal of Internet and Enterprise Management*, *6*(4), 279–314.

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security*, *39*(0), 396–405.

Boonstra, A., & Broekhuis, M. (2010). Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. *BMC Health Services Research*, *10*, 231.

Brady, J. (2011). Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. In *System Sciences (HICSS), 4,* 1–10. IEEE.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Comp Security*, *22*(5), 474–489.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207.

Donahue, S. E. (2011). *Assessing the impact that organizational culture has on enterprise information security incidents*.

Gaunt, N. (2000). Practical approaches to creating a security culture. *International Journal of Medical Informatics*, *60*(2), 151–7.

Gebrasilase, T., & Lessa, L. (2011). Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. *African Journal of Information System*, *3*(3), 72–86.

Ghernouti-Hélie, S., Tashi, I., & Simms, D. (2010). A Multi-stage Methodology for Ensuring Appropriate Security Culture and Governance. *ICARS*, 353–360. IEEE.

Granlien, M. S., & Hertzum, M. (2012). Barriers to the Adoption and Use of an Electronic Medication Record. *The Electronic Journal Information Systems Evaluation*, *15*(2), 216–227.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*(1), 242–251.

Hagen, J. M., Albrechsten, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Info Mngmt and Comp Security*, *16*(4), 377–397.

Hedstrom, F. ;, & Karin, K. (2014). End User Development and Information Security Culture. In *HCI Int. Conference on Human Aspects of Information Security Privacy and Trust*, 1–12.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies : The Critical Role of Top Management and Organizational Culture. *Desicion Science*, *43*(4), 615–660.

Ifinedo, P. (2014). The Effect of National Culture on The Assessment of Information Security Threats. *International Journal of Electronic Business Management*, *12*(2), 75–89.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Joint Technical Report, Computer Science Dept, Keele, UK, Keele Univ (TR/SE- 0401) and National ICT Australia Ltd.*

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology*, *51*(1), 7–15.

Knapp, K., & Marshall, T. (2006). Information security : management ' s effect on culture and policy. *Information Management & Computer Security*, *14*(1), 24–36.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, *28*(7), 509–520.

Lopes, I., & Pedro, O. (2014). Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises. In *New Perspectives in Info Systems and Technologies*, 277–286.

Mansouri-Rad, P., Mahmood, M. A., Thompson, S. E., & Putnam, K. (2013). Culture Matters: Factors Affecting the Adoption of Telemedicine. *Hawaii Int.Conf.on Syst Sc* (pp. 2515–2524). IEEE.

Martins, A., & Elofe, J. (2002). Information Security Culture. *Safety in the Info Society*, 203–214.

Martins, N., & Veiga, A. (2010). The Value of Using a Validated Information Security Culture Assessment Instrument. *European Conference on IS Management and Evaluation*, 146–154.

Merhi, M. I. (2014). *Creating an information systems security culture through an integrated model of employees compliance*. University of Texas-Pan American.

Ngo, L., Zhou, W., Chonka, A., & Singh, J. (2009). Assessing the level of I.T. security culture improvement: Results from three Australian SMEs. *Industrial Elect Conf.*, 3189–3195.

Okere, I., Niekerk, J. van, & Carroll, M. (2012). Assessing Information Security Culture: A Critical Analysis of Current Approaches. In *Information Security for South Africa*, 1–8.

Omachonu, V., & Einspruch, N. (2010). Innovation in healthcare delivery systems: a conceptual framework. *The Innovation Journal: The Public Sector Innovation Journal*, *15*(1), 1–20.

Ramachandran, S. (2008). Information security cultures of four professions: A comparative study. In *41st Hawaii International Conference on System Sciences*, 1–10.

Sabbagh, B. A., & Kowalski, S. (2012). Developing social metrics for security modeling the security culture of it workers individuals (case study). *MIC-CCA 2012 Mosharaka*, 112–118.

Salleh, N., Mendes, E., & Grundy, J. (2011). Empirical Studies of Pair Programming for CS/SE Teaching in Higher Education: A Systematic Literature Review. *IEEE Trans on Software Engineering*, *37*(4), 509–525.

Samy, G. N., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal*, *16*(3), 201–9.

Schlienger, T., & Teufel, S. (2005). Tool supported management of information security culture. In *IFIP Advances in Information and Communication Technology*.

Shaaban, H., & Conrad, M. (2013). Democracy, culture and information security: a case study in Zanzibar. *Information Management & Computer Security*, *21*(3), 191–201.

Shahibi, M. S., Rashid, R. M., Fakeh, S. K. W., Dollah, W. A. K. W., & Ali, J. (2012). Determining Factors Influencing Information Security Culture among ICT Librarian. *JATIT*, *37*(1), 132–140.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486.

Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Comp & Security*, *49*(2015), 162–176.

Vroom, C., & Solms, R. Von. (2004). Towards information security behavioural compliance. *Computers & Security*, *2004*(23), 191–198.

Williams, P. A. H. (2009). Capturing Culture in Medical Information Security Research. *Methodological Innovations Online*, *4*(3), 15–26.

Woodhouse, S. (2007). Information Security: End User Behavior and Corporate Culture. In *7th IEEE International Conference on Computer and Information Technology*,767–774.

Zakaria, O. (2006). Internalisation of Information Security Culture amongst Employees through Basic Security Knowledge. *Security and Privacy in Dynamic Environments*, *201*, 437–441.