Journal of Theoretical and Applied Information Technology
20th June 2016. Vol.88. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INFORMATION SECURITY CULTURE IN HEALTHCARE INFORMATICS: A PRELIMINARY INVESTIGATION

[1]NOOR HAFIZAH HASSAN, [2]ZURAINI ISMAIL

[1] Department of Information System, Universiti Tenaga Nasional, Malaysia

[2]Assoc. Prof., Department of Information Security, Universiti Teknologi Malaysia, Malaysia

E-mail: [1]hafizah@uniten.edu.my, [2]zurainiismail.kl@utm.my

ABSTRACT

Information security culture becomes an enabler towards an effective security practice. Human factors are recognised as one of the factors in addressing the issue of information security in healthcare informatics. Inculcating information security culture among healthcare practitioners is identified to be one of the solutions for a better security practice. Thus, identifying the issues and factors that influence information security culture are important. A preliminary investigation involving six healthcare professionals and academics have been carried out for better understanding on the critical factors that may influence the information security culture. In-depth interview method is chosen in this study. Thematic coding was conducted to characterise the themes and asses the factor that found to be influential. Results from the in-depth interviews with healthcare expertise showed that four main themes may influence the degree to which information security may be cultivated. Security behaviour, security value, security awareness, and enforcement of security policy are the themes addressed by the key informants as the influential factors inculcating information security culture. This study also found that various level of healthcare professional exhibited different outcomes in information security culture. Findings from this study may provide guidance to the healthcare organisation to ensure their employee inculcate information security culture in holistic manner.

Keywords: *Information Security Culture, Healthcare Informatics, Organizational Culture, Information Security, Healthcare*

1. INTRODUCTION

Information security underpins profitability and commercial viability towards achieving effectiveness in organisations. In current health informatics environment, healthcare informatics has the greatest potential for improving quality in healthcare by providing a wide-range of capabilities. The innovations in health informatics allow the implementation of its functionality to be constituted of a significant quality enhancement among health practitioners [7]. Health informatics and structured accessible secure data captured provide effectiveness in information security management system. This innovation makes previously established ways of doing work in healthcare information system to become outmoded. Despite the potential for quality improvement, the concerns about the privacy and security of patient's data are viewed as a barrier to the usage of healthcare informatics [8], [9].

Many healthcare organisations have been negatively affected by security threats and data thefts [10], [11]. Security vulnerability heightens as many administrative and clinical tasks depend on healthcare informatics to support healthcare organisation business operation [12]. Furthermore, securing patient information becomes one of the pressing issues in current health care provision [13]. To overcome this crisis, security regulation is needed to ensure patient privacy and confidentiality. Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted with the purpose to improve quality care and the continuity of health insurance coverage that leverages on information technology (IT) in European countries. In this case, Malaysia uses the ISO2007:1 for establishing standards in security regulation through Personal Data Protection (PDPA) act which came into force starting 15th November 2013 with the objective to protect patient data and ensure privacy. In compliance towards ISMS ISO2007:1, the information security policy was regulated in most healthcare organisations. The

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

purpose of having these established rules in addressing specific security issues is to provide a framework of instructions on what the employee should do when dealing and interacting with information technology as well as to provide a basis for the practices to be reviewed regularly [14].

Despite of having security regulations, the employee is identified as the weakest link in information security in an organisation [15]. Information security culture is recognised as having as an influence towards end-user compliance towards information security controls and policies in the organisation. According to scholar is [16], information security culture can be formed by instilling the identified aspects of information security on each employee to make it as a natural way on executing their daily job in an organisation. Literature has agreed that cultural belief can be found to influence behaviours among members of a profession that distinguish them in the organisational system and profession that they belong to. Thus, these phenomena have led towards the investigation and understanding of determinants inculcating information security culture in healthcare organisations. Indeed, it is important for scholars to understand and determine factors that contribute towards the success of a prescribed information security culture. It also can provide an insight into different professional groups in healthcare organisations that is necessary to understand the security-related beliefs of their members in implementing the information security management system.

This paper aims to explore and understand the influencing factors of security culture in healthcare informatics through preliminary investigation. This paper is organised into five sections. The first section is introduction, followed by the details about information security culture in health informatics. The third section describes the research methodology. Then, the fourth section elaborates in details the outcomes from in-depth interviews. The last section summarises the discussion and suggestion for future research.

2. INFORMATION SECURITY CULTURE IN HEALTHCARE INFORMATICS

According to the statistics from Ponemon Institutes in United States, 43% of data breaches were accounted from healthcare organisations. Besides, according to Symantec Threat Report of 2014, the top three major attacks on computer networks through phishing and malware were reported in healthcare organisation. In addition, attacks of servers in hospital are increasing within the healthcare facilities used by the hospitals as doctors often discard private information without fully deleting them, exposing them to identity thefts. The issues of information security management becomes more important when the information system pervasively underpin the operation of an organisation and as the operation solely depends on their information system; such as those practiced in healthcare organisation [4]. Information security management focuses on developing and maintaining the security control of the organisation. However, most of the researches in information security management focused on financial and electronic commerce [9]–[11] compared to health informatics area. Having said that, a growing concern of research in information security can be observed in understanding the factors that influence information security culture that may contribute towards successful implementation of information security management in health informatics [12].

Healthcare practitioners and management have very different experiences in expressing a strong need for a better organised approach towards promoting information security culture. Managements are the key points that support healthcare practitioners in inculcating security culture. There are arguments on how information security culture can be promoted as part of an essential organisational culture. Knapp & Marshall (2006) stated that security culture needs to be separated from organisational culture for the reason that each organisation has their own unique role and business purpose. As for healthcare organisation, this view must be investigated to suit it with the organisation's business purpose and goal. Meanwhile, in healthcare organisations one of the elements which is identified as trust is known to be embedded when conducting research related to medical information security culture research [5]. Furthermore, no specific model was designed to adjust the needs and requirements of healthcare organisations in relation to the inculcation of information security culture through health informatics.

Information security cultures and practices occur more vigorously in developed countries because of the recognition of the importance of information security and how it has an impact on the reputation, financial loss, and business confidence in an organisation. One of the commonly reported scenarios that can happen in health informatics is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

when assets such as a pen drive or computer is left unattended with a consequence of the loss of medical report results [14]. Therefore the need to raise awareness towards security in developed countries to ensure their work environment in a safe culture has been made compulsory to safeguard confidentiality. However, the majority research works on information security culture were performed in Finland [15], South Africa [16], Saudi Arabia [17], Australia [18], [19], and Switzerland [20]. Malaysian information technologies are still at the development phase with information security and management concern revolving on how to create a security conscious culture towards achieving Vision 2020. Thus, addressing the factors influencing information security culture can bridge the gaps in creating security conscious culture in Malaysia.

Within the last few years, research in this new area of information security culture has grown rapidly. However, most of the research focused on attitude and behaviour [17], [21], adopting Schein Model [20], [22]–[24], organisational culture context [25], information security principle [13] and on improving the aspects of security culture towards adherence of security policies [26]. Furthermore, recent study in [17] has conceptualized the context of information security culture towards the behaviour of the users. Recent research of cultural factors in security awareness also covered on [28] by stating that cultural change is important before the organisation can implement ISMS.

Lack of a single model that integrates the factors identified from previous literature motivates this research. Hence, this research integrates the factors that have previously been identified into one single model as the determinants of information security culture by employing theoretical perspective that underpins information security culture. Educating employees on ethics in information technology can be done through the organisation by emphasising on the important factors influencing information security culture.

Another study conducted by [18], revealed that there are significant differences in belief and values on group of profession in organisations. Thus, identifying values on beliefs related to information security can assist in understanding the concept of security culture. No single research has mention on how different professions of healthcare practitioners inculcate information security culture.

3. RESEARCH METHODOLOGY

Preliminary investigation was carried out for this research to seek out the influential factors of information security culture in healthcare informatics. The preliminary investigation was under-taken in Malaysia with a different background of key informant. The key informants were selected based on their experience by using any related system on healthcare informatics, the involvement of development of hospital information system or conducting researches on HIS and in information security policy development in Malaysia. The research procedure involved voluntary cooperation with the purpose of the study has been briefed to the key informants. In this process, Six (6) key informants were involved and in-depth interviews were conducted with them. Each session took 30 minutes to 1 hour. The key informants' details that are involved in this preliminary investigation are depicted in Table-1. Each of the key informants is labelled to K1, K2, K3, K4, K5, and K6 accordingly.

Table 1: Key Informants' Detail on Preliminary Investigation

Designation	Specialisation	Organisation	Years
Academician (IT) (K1)	HIS User	University	13
Medical Doctor (K2)	HIS User	Hospital	4
Academician (IT)(K3)	HIS User	University	12
Academician (IT) (K4)	Healthcare	University	14
IT Specialist (K5)	HIS security policy developer	Government Sector	4
HIS System Analyst cum Academician (IT) (K6)	HIS developer	Hospital	14

This study employs three important processes following [6] in analysing the in-depth interview which are describe in Figure-1. The processes are data reduction, data display, and follow up by conclusion. This process is implemented to ensure that the themes emerged was validated properly. Atlas.ti is the software used in qualitative data analysis.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

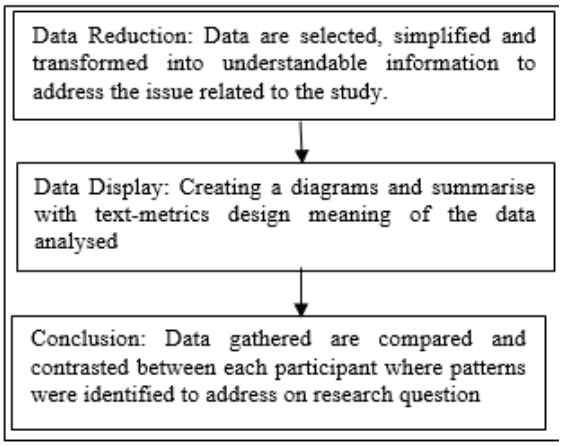

Figure 1: Analysis of In-depth Interview

The in-depth interviews were conducted based on research questions derived from previous study on information security culture [15], [19], [20] as listed in Table-2. The interview constructs items were chosen as information security culture is a relatively new area that still ambiguous in terms of its own definition [21].

Table 2 depicted the interview construct and relevancy that shows justification on why the interview question was constructed. From the preliminary investigation, the discussion on the interview outcomes is divided according to the research question developed in the next section.

Table 2: Interview Constructs Item

Interview Constructs	Relevancy
1. What are the importance of information security in your organisation and your daily work routine?	To identify different type of security threat in healthcare organisation based on their experience. [10], [22] emphasizing different threat categories occurred in health informatics.
2. What are related issues and barriers on security in healthcare information system that you want to highlight that might need to be explored in future research?	To understand resistance factors that need future exploration as security threat is increasing in health informatics [23].
3. What would you do and implement to ensure you and your employee inculcating information security culture?	To recognise whether the key respondents know the terms of information security culture as the terms still in ambiguity [21].
4. What is your current concerns regarding ICT security culture levels?	To explore their experience and security knowledge accordingly according to their profession level.

4. DISCUSSION ON INTERVEIW OUTCOMES

Research Question 1: What are the importance of information security in your organisation and your daily work routine?

Information security is definitely important to the key informants. However, they describe the importance of information security in their own perspectives. Most of them agree that importance security should be stored as a value among them. Four (4) of them confirmed this by saying that:

"Information security is important up to the value of daily routine work, however we did not emphasise on information security at all as" (K2)

"We found out that information security is important, however, this is depends on the seniority level of user using the hospital information system" (K6)

"Of course it is important, however, they must be a reminder or message that need to be send to the employee to ensure that they follow the security procedures that have been guided in the organisation" (K5)

Thus, from the first question, we may conclude that emphasisation or value of security on each of the employee should be embedded through their daily routine. It aligned with the research in [24], on what they said that value is important to the employee use to interact with the organisation's systems and procedure at any point in time.

Research Question 2: What are related issues and barriers on security in healthcare information system that you want to highlight that might need to be explored in future research?

During the interview session, the key informants get confused with the terms of information security culture. Instead, they highlighted the issues they faced with healthcare information system.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

"Basically, if you want to touch about security, you must ensure that our hardware equipments are working properly as we had experienced most of the hardware are not well maintained" (K2)
"There are few people in the organisation that have their own views, and to make sure that they adhere to the security initiatives, the current healthcare organisation must be able to create a conscious security culture in the organisation" (K1)
"If you want to look in healthcare informatics you must be able to look in the patient privacy" (K4)
"Resistance of the people or professionals who want to make use of healthcare information system also are important as we need to educate them as much as we can" (K5)

Key informants constantly keep abreast of the reliability of the hardware equipment in the current healthcare organisation that needs to be improved. In this section, we know that in order for us to create an information security conscious culture, there is a need to maintain the related information technology hardware, and tool equipment in the organisation itself.

Research Question 3: What would you do and implement to ensure you and your employee inculcating information security culture?

From this research question, the intention is to get the key informants which are the idea on how they can motivate themselves to cultivate information security culture. It seems that most of them agree that awareness is the most important thing to highlight when inculcating information security culture. They convey their message such as:
"You should look into awareness of the people regarding information security…." (K1)
"My previous research touches on the values of the people in the organisation, you should look into the awareness of the people in the organisation on how can we make sure that they are aware of security as most of them did not know the existence of information security?" (K4)
"We have hired few people outside Malaysia in developing our system. We need to educate our people or the employees in the organisation in a proper way, maybe through knowledge management?" (K3)
"The importance of raising security awareness are the issues that need to be highlighted from the lowest level until the upper level, and we have provide training and security awareness to them but I think it is not enough as I do not see the technical factor is considered as important in this stage" (K5)
"Different attitude and behaviour of employees in the organisation are important as they sometimes tend to do what they feel good for them" (K6)

They highlighted that top management has follow certain procedure to ensure that all the members are keep updated on information security. Some of them go to various security seminars. In terms of HIS user aspects, they tend to highlight the awareness that must be embedded in the employees in a creative way. Apart from that, one of them highlighted the attitude and behaviour of the employees in the organisation also play an important role to the information security itself as well as to the other employee. It confirmed the findings from [4], they found out that security awareness and security behaviour are the two most important parts that need to be highlighted in information security culture among healthcare professional. One of them also highlighted that different level of profession provides different level of security level of thinking. It is similar to the findings by [18], in investigating different security values among different profession that exhibit various security levels.
Thus, this research conclude that security behaviour and security awareness are the important criteria that need to be highlighted in inculcating information security culture.

Research Question 4: What is your current concerns regarding ICT security culture levels?

Following the importance of top management in managing their employee security culture as in [20], this research question has been constructed. Their finding showed that top management has play some of their role to ensure that information security has been put in a proper place. Three (3) of the key informants described this view by:
"Top management have highlighted many times the information security culture through security policy, however there is no initiatives from the employee itself" (K1)
"I never see any information security guidelines in any websites or any poster on how you can control on security…." (K3)
"When you talk about security in healthcare informatics, you must know how to differentiate between privacy and security control that must be emphasized by the organisation such as security policy" (K3)
"I have listed out many types of hospital information system implementation in my research; however I could not see the effectiveness of the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

system, yet security issues are rarely being explored in this research. Maybe you want to look on how to implement effective security strategy, maybe should focus on overall goal of the organisation" (K4)

In the outcomes, they stated that the needs of information security strategy from the organisation must be highlighted to ensure that they cultivate information security culture. One of them highlighted the existence of security policy that needs to be enforced to every level of employee in the organisation. Hence, we can conclude that information security policy enforcement is important to ensure information security culture can be cultivated. This outcome align with the findings from [15] that highlighted the importance to put security policy enforcement in a proper place.

5. FINDINGS

The interview outcomes were analysed and visualized in Figure-2. The themes derived from the interviews are identified as factors that influencing information security culture in healthcare informatics. Four (4) themes have been identified that may influence the information security culture in healthcare informatics. This are security behaviour, security awareness, security values, and enforcement of information security policy. These themes will be used to design a conceptual model that shows factors inculcating information security in healthcare informatics. From in-depth interview conducted, this research summarise that security behaviour, security awareness, security values, and enforcement of information security policy is positively related with information security culture.

The first emerging theme found in this study is security behaviour. This study align with the finding from the context of security behaviour in [19]. They emphasised that security behaviour may help to cultivate security culture if the appropriate information security components is identified. In their study, information security components are treated as the input that influence employee to exhibit certain security behaviour in the organisation. Therefore, security behaviour are evolving with time together with the things are implemented in the organisation, thus cultivate information security culture [25]. Secondly, the next theme identified is security awareness. The key informants agree that security awareness must be emphasize as one aspect of their daily work routine. Moreover, security awareness is identified as one of the components that must be instilled in each employee to ensure that security attacks are thwarted; ensuring organisational assets and reputation remain secure [26].

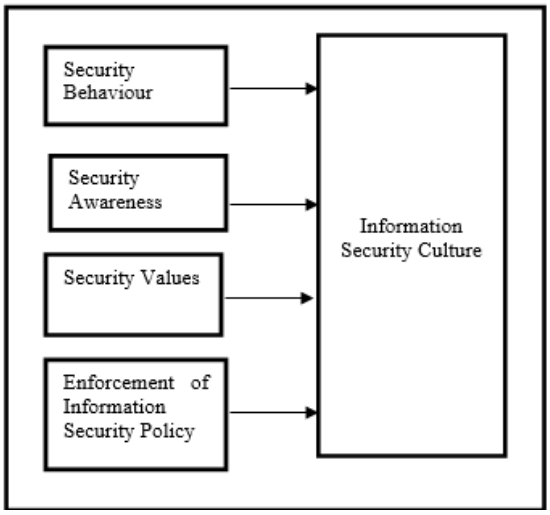

Figure 2: Emerging Themes from Interview Outcomes

Meanwhile, the third themes which is security value serve as principle of employee in the organisation that may comprises as their belief and assumption. In higher education for instance, cultural assumption and belief were found to be the most influential factors affecting security awareness thus affecting security culture [26]. In [27], they claimed that employees in healthcare would be motivated towards manifesting what they belief in the actions they perform. Furthermore, in [28], they found that principles formed as beliefs in individuals significantly influence information security culture. In this study, the context of cultural assumption and belief will be referred as security values. Furthermore, different background of professions may offer different security culture[18].

The fourth theme emerged from this study is enforcement of information security policy. Based on the interview conducted earlier, they assumed that by having an appropriate information security policy in the organisation, the tendency of information security culture to be cultivated will increased. Furthermore, from study conducted in [29], they found that policy enforcement is the most significant factor influencing security culture. This support the last theme identified in this study. The interaction between information security components such as policy of the organisation the behaviour of employees have a positive impact on resulting information security culture.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6. CONCLUSION

This on-going research has demonstrated initial findings based on a preliminary investigation conducted through in-depth interview. From the in-depth interview conducted with six respondents, four research questions have been answered. This may provide a significant view from different type of key informants' background. The first interview construct item summarised that the importance of information security should put in high priority. Meanwhile, the second interview items describe they are having human and organisational issues in using healthcare information system. In the third interview items, the direction of research in information security culture is identified. Even though only one respondent stated that cultural changes are the most important things to look at in information security, it has strengthen the area that needs to be explored in information security culture. For the fourth interview items, it can be concluded that information security culture is relatively new in healthcare information system since three of the respondents agree that they are not aware of security culture term in Malaysia. Hence, it can be concluded even though they found out that information security are important, they tend to ignore it in their daily work routine. They should embed security value in their workplace. It can be concluded that with an appropriate security behaviour program along security awareness seminar and training, it may help the employees to cultivate information security culture. Nevertheless the enforcement of security policy is important in emphasising and embracing information security culture in healthcare informatics.

The limitation of this study is the ethical consideration involved in conducting data collection in healthcare organisation. This study should also cover different perspectives of various healthcare professional backgrounds. Hence, with the supports from literature, the next phase can be proceeded with the development of conceptual model derived from themes emerged from this study. It follows with the validation process of the proposed model in government supported hospital. This paper has described as an initiative of exploring the critical area and factors inculcating information security culture in healthcare informatics. The findings for this study may be beneficial for healthcare organisation by inculcating information security culture before implementing information security management system.

REFERENCES:

[1] A. Alhogail, "Design and Validation of Information Security Cultural Framework," *Comput. Human Behav.*, vol. 49, pp. 567–575, 2015.

[2] H. Kruger and S. Flowerday, "An assessment of the role of cultural factors in information security awareness," *Secur. South Africa ,* vol. 13, no. 4, pp. 195–201, Nov. 2011.

[3] A. Veiga and N. Martins, "Improving the information security culture through monitoring and implementation actions illustrated through a case study," *Comput. Secur.*, vol. 49, no. 2015, pp. 162–176, 2015.

[4] T. Gebrasilase and L. Lessa, "Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital," *African J. Inf. Syst.*, vol. 3, no. 3, pp. 72–86, 2011.

[5] P. A. H. Williams, "Capturing Culture in Medical Information Security Research," *Methodol. Innov. Online*, vol. 4, no. 3, pp. 15–26, 2009.

[6] M. B. Miles, M. Huberman, and J. Sladana, *Qualitative Data Analysis; a Methods Sourcebook*, vol. 28, no. 4. 2014.

[7] A. D. Black, J. Car, C. Pagliari, C. Anandan, K. Cresswell, T. Bokun, B. McKinstry, R. Procter, A. Majeed, and A. Sheikh, "The impact of ehealth on the quality and safety of health care: A systematic overview," *PLoS Med.*, vol. 8, no. 1, pp. 1–16, 2011.

[8] M. S. Granlien and M. Hertzum, "Barriers to the Adoption and Use of an Electronic Medication Record," *Electron. J. Inf. Syst. Eval.*, vol. 15, no. 2, pp. 216–227, 2012.

[9] A. Boonstra and M. Broekhuis, "Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions.," *BMC Health Serv. Res.*, vol. 10, p. 231, 2010.

[10] 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.

[11] S. Tritilanunt and A. Tongsrisomboon, "Risk Analysis and Security Management of IT Information in Hospital," *Int. J. Comput. Inf. Technol.*, vol. 4, no. 2, pp. 1–9, 2014.

[12] R. Gomes and L. V. Lapão, "The adoption of IT Security Standards in a Healthcare Environment," *Stud. Health Technol. Inform.*, vol. 136, pp. 765–770, 2008.

[13] J. I. Fernando and L. L. Dawson, "The health information system security threat lifecycle: an

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

informatics theory.," *Int. J. Med. Inform.*, vol. 78, no. 12, pp. 815–26, Dec. 2009.

[14] W. S. Park, S. W. Seo, S. S. Son, M. J. Lee, S. H. Kim, E. M. Choi, J. E. Bang, Y. E. Kim, and O. N. Kim, "Analysis of information security management systems at 5 domestic hospitals with more than 500 beds," *Healthc. Inform. Res.*, vol. 16, no. 2, pp. 89–99, 2010.

[15] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empiracal Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2010.

[16] J. Van Niekerk and R. Von Solms, "A holistic framework for the fostering of an information security sub-culture in organizations," in *Information Security for South Africa 2005*, 2005, pp. 1–13.

[17] A. AlHogail, "Design and validation of information security culture framework," *Comput. Human Behav.*, vol. 49, no. 2015, pp. 567–575, 2015.

[18] S. Ramachandran, "Information security cultures of four professions: A comparative study," in *41st Hawaii International Conference on System Sciences*, 2008, pp. 1–10.

[19] 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, Mar. 2010.

[20] K. Knapp and T. Marshall, "Information security : management ' s effect on culture and policy," *Inf. Manag. Comput. Secur.*, vol. 14, no. 1, pp. 24–36, 2006.

[21] D. Oost and E. Chew, "Investigating the Concept of Information Security Culture," 2007.

[22] G. N. Samy, R. Ahmad, and Z. Ismail, "Security threats categories in healthcare information systems.," *Health Informatics J.*, vol. 16, no. 3, pp. 201–9, Sep. 2010.

[23] R. G. Fichman, "The Role of Information Systems in Healthcare : Current Research and Future Trends," *Inf. Syst. Res.*, vol. 22, no. 3, pp. 419–428, 2011.

[24] N. Martins and A. Veiga, "The Value of Using a Validated Information Security Culture Assessment Instrument," in *8th European Conference on IS Management and Evaluation*, 2010, pp. 146–154.

[25] L. Ngo, W. Zhou, and M. Warren, "Understanding transition towards information security culture change,"*3rd Australian Information Security Conference,* 2005, pp. 1–6.

[26] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," *Comput. Secur.*, vol. 27, no. 7–8, pp. 241–253, 2008.

[27] N. Humaidi and V. Balakrishnan, "The Influence of Security Awareness and Security Technology on Users ' Behavior towards the Implementation of Health Information System : A Conceptual Framework," *ipedr.com*, vol. 35, pp. 1–6, 2012.

[28] M. S. Shahibi, R. M. Rashid, S. K. W. Fakeh, W. A. K. W. Dollah, and J. Ali, "Determining Factors Influencing Information Security Culture among ICT Librarian," *J. Theor. Appl. Inf. Technol.*, vol. 37, no. 1, pp. 132–140, 2012.

[29] M. Alnatheer, T. Chan, and K. Nelson, "Understanding And Measuring Information Security Culture," in *Pacific Asia Conference on Information Systems (PACIS) 2012*, 2012, p. 144.