INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 8, Issue 11, (2018) E-ISSN: 2222-6990

Exploring User's Experience using E-Notification Management System

Norshima Humaidi, Vimala Balakrishnan, Melissa Shahrom

[1,3]Faculty of Business and Management, Universiti Teknologi MARA Selangor, Puncak Alam Campus, Malaysia

[2]Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia

Corresponding Author Email: [1]norshima958@puncakalam.uitm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v8-i11/5282 DOI:10.6007/IJARBSS/v8-i11/5282

Published Date: 08 December 2018

ABSTRACT

Technology is believed to give an impact on user's behaviour. Thus, e-notification management system prototype was developed to improve user's compliance behaviour towards Information Security Policies (ISPs). The purpose of this study was to evaluate how this prototype can be used to improve the security compliance behaviour among users through their experience of using the propose system. Eighteen (18) users from selected local hospitals in Malaysia were interviewed and the qualitative analysis found that Management Support, Information Security Awareness, Self-Efficacy, Security Barrier and Trust contributed to ISPs compliance behaviour. Furthermore, most of the participants were satisfied with the prototype system. The prototype is hoped to give benefits to organizations in implementing and distributing ISPs systematically, especially in healthcare sector.

Keywords: Prototype, Notification Management System, User's Compliance Behavior, Information Security, Information Security Compliance Behaviour.

INTRODUCTION

Effectiveness of Information System (IS) security can be achieved through promoting adequate information security behaviour and constraining unacceptable information behaviour among employees in the organization (Bélanger, Collignon, Enget, Negangard, 2017). Moreover, if user's compliance behaviour towards information security is acceptable, security incidences can be decreased, and the effectiveness of IS security can be increased (Bauer, Bernroider & Chudzikowski, 2017). This is also supported by other information security studies that stated that security compliance behaviour can promote security assurance behaviour, such as employees will be more careful in handling an organization's data (Rocha Flores, Antonsen, & Ekstedt, 2014; Guo, 2012).

Previous studies describe information security compliance behaviour as behaviour that does not violate an organization's ISPs (Guo, 2012) and adheres to a set of core information security activities as recommended by the organization (Padayachee, 2012). Most of the ISPs are developed from the security requirements in an organization to suit their own objectives (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). Organization's ISPs usually consists of several focus areas such as password management, information handling, security incidents reporting, among others (Parsons et al., 2014). The ISPs cannot be implemented effectively if the employees do not know or aware about it. Thus, it is necessary that the ISPs are correctly and appropriately deployed throughout the organization and actually brought to all employees (Höne & Eloff, 2002).

According to Hone and Eloff (2002), the distribution of ISPs can be done during information security training using full paper based or electronic copies of the documents, through publishing the document on internal website. An effective information security programme could increase user awareness towards information security and promote good user information security behaviours (Bauer et al., 2017; Ng, Atreyi, & Yunjie, 2009). If users are not motivated to follow organization's rules and procedures to protect information, security might fail; hence, management play an important role to ensure the effectiveness of information security programme (Waly, Tassabehji, & Kamala, 2012) and influences employee's compliance behaviour towards ISPs (Norshima Humaidi & Vimala Balakrishnan, 2017). Based on the previous reviews, there is no study propose a system to alert ISPs in a systematic way; however, the previous studies argued that management support and information security awareness are the significant factors of security compliance behaviour (Norshima Humaidi & Vimala Balakrishnan, 2017; Brady, 2011). Therefore, this study was conducted to develop a prototype that can be used to distribute and notify users about information security programme and policy based on the significant factors discussed above, namely HIS notification prototype. Moreover, this study also was aim to evaluate how the proposed prototype can be used to improve user's compliance behaviour towards ISPs in the context of Malaysian healthcare sector.

RESEARCH METHOD

Research Design

Qualitative research was employed to collect and analyse the interview data during the prototype testing phase. The prototype testing is the stage in which the prototype will be tested by end-users. The prototype was developed based on the significant factors in Health Information System Security Policies Compliance (HISSPC) model that were found during the hypotheses testing (quantitative analysis) (Norshima Humaidi & Vimala Balakrishnan, 2017). The purpose of prototype testing is to further evaluate the HISSPC model in explaining users' compliance behaviour towards IS security policies through the users' experience of using the proposed system.

Data Collection

The data collection began by selecting typical sample as a method to choose the participants that were involved in this study. For this reason, the main participants that were involved included the health professionals responsible in keeping and managing patient's health records using Health Information System (HIS) such as doctors, pharmacist and nurses. These health professionals were believed to have wide knowledge and experience on the

process of managing health records using HIS. This study also interviewed several health administrators who handled health records. The types of sampling method that has been adopted for qualitative research in this study was snowball sampling.

Semi-Structured Interviews

The interviews were conducted once the users completed the testing process. Interviews were chosen as they are able to provide depth to a particular issue. The interviews were recorded on audio tapes and transcribed after the interviews ended.

The interview questions were semi-structured and allowed open-ended responses. However, the open-ended responses were controlled to ensure that the interview topics were covered and do not go beyond the research scope. Through these interviews, information was collected pertaining to users perception towards complying with health information system security policies and their perceptions towards the current module of the HIS prototype that might help to improve compliant behaviours towards ISPs. The semi-structured interviews were guided by a set of two open-ended questions that served as a data collection guide. The open-ended questions were self-developed and during the interview section, no questions were deleted. A total of 18 participants participated in the prototype testing and interviews.

Data Analysis

In this study, we used the thematic analysis approach to analyse the interview data to achieve research objective. The thematic analysis is a foundational method in qualitative analysis to search for themes or patterns from interview data. The qualitative data analysis tool used in this study was ATLAS.ti version 7.1 to analyse and organise interview data.

Additionally, Subject Matter Experts (SMEs) were reviewed the qualitative analysis as a means of independent verification regarding the logic and theoretical structure of the themes, sub-themes, and the institutional story constructed.

E-NOTIFICATION MANAGEMENT SYSTEM PROTOTYPE REQUIREMENTS

The requirements of the e-notification management system prototype modules were identified based on the significant factors of HIS security compliance behaviour model (Norshima Humaidi & Vimala Balakrishnan, 2017) as shown in Figure 1. The research model found that Management Support (Leadership Behaviour) influenced user's information security awareness and compliance behaviour towards HIS security policies. Moreover, information security awareness (Severity Awareness and Benefit of Security-Countermeasure Awareness) also influenced user's information security compliance behaviour towards HIS security policies.

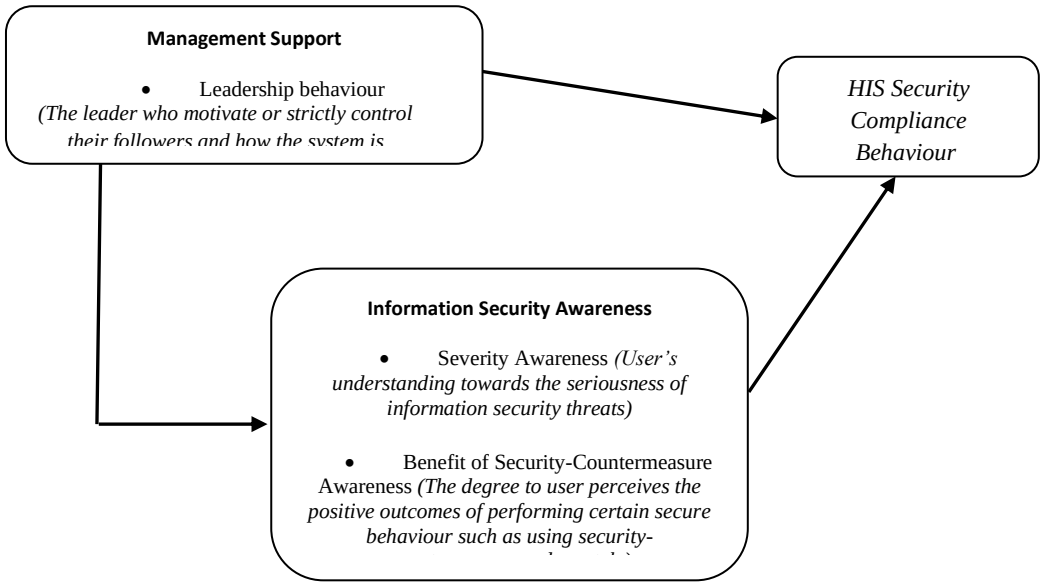

Figure 1: HIS Security Compliance Behaviour Model

PHP scripting language version 5.3 was used for the programming or logical design of the prototype system. The prototype requirements focused on the indicated significant factors as shown in Table 1.

Table 1:
The significant factors and prototype modules

Significant Factors	HIS E-Notification Modules	Current HIS
Management Support	Manage for users to receive and read online announcement messages/notifications.	Current procedure use internal email to alert and distribute HIS security policies and other news that related with security policies.
	Manage any information updated related to HIS security policies, information security threats and HIS training.	
	Manage Short Message System (SMS) configuration.	
Information Security Awareness	Receive online announcement messages and SMS notification: • ISPs announcements • Information security threat alerts • E-Training	Not available in current HIS.

RESULTS

Prototype Testing

The prototype testing was carried out in two stages. In the first stage, the researcher ran system testing to test the system functionality. The system testing involved two modules: IT administrator module and HIS user module. The results of the system testing showed that all the prototype modules were run successfully. The connection to the system was also successful without any problem.

In the second stage, the HIS user module was tested by HIS users to determine whether the proposed module is effective to improve users' compliance behaviour towards ISPs related with HIS uses. At this stage, the data was collected using the qualitative technique.

Participants Profile

All the participants selected in the interview section were HIS users from different positions. This is because some employees may be more aware or sensitive to certain issues than other employees, as each of them holds a unique position that can influence their experience and perceptions. Table 2 presents the profiles of the interviewees for this study.

Table 2:
Participants profile

Demographic	Hospital A	Hospital B	Hospital C	Total (n = 18)
Position				
Doctor	3	1	2	6
Support Staff	2	2	3	7
Health Record Administrator	0	2	3	5
Gender				
Male	1	1	1	3
Female	4	4	7	15
HIS Usage Experience				
More than 5 years	1	2	4	7
Less than 5 years	4	3	4	11

The participants profile (Table 2) shows that there are five participants in the Hospital A and Hospital B, and eight in the Hospital C. The majority of the participants were support staff (nurses, pharmacists, radiologists, etc.) with the total number of n = 7, female (n = 15) and experience of using HIS for more than five years (n = 11). Each of the participants was interviewed via one-to-one interviews in the office at the particular hospital that the employee works for the purpose of tracking their perceptions towards the issue. Each interview lasted about 1 hour. By using an interpretive approach – assuming the interviewee's role, moving from the parts to the entire interview data, and identifying common patterns – the researcher was able to delineate certain dimensions. More importantly, the qualitative findings were able to explain users' compliance behaviour towards HIS security policies.

Qualitative Results Findings and Interpretation

The sub-themes were developed through the coding process from the content of the interviews. The sub-themes were divided into several categories that became primary themes for this study. Most of the primary themes (Management Support, Perceived Severity, Perceived Susceptibility and Perceived Benefit) were also shown to be significant factors that

influenced the users' compliance behaviour towards HIS security policies. The summaries of the qualitative theme findings are shown in Table 3.

Table 3:
Summary of qualitative themes

Participant Code	Quotation	Sub-Theme	Theme
P11	*"If new policies are implemented, the top management will email the information to our head of department (HOD), and then the HOD will forward the email to us."*	Leadership behaviour	Management Support
P1	*"We can retrieve the ISPs through the hospital intranet portal. We can also view the ISPs document online. My concern is that the hospital management was not informed about information security incidents or threats formally. So, I was not aware about this."*	ISPs implementation	Management Support
P7	*"If anything happens to my computer or the system itself, I will refer to the IT staff and ask them to solve the problem. For example, I was careless when keying in patients' data, and wrong data were keyed into the system. As I had difficulty recovering it, I asked the IT staff to retrieve the data and correct it."*	Skill	Self-Efficacy

P12	*"I understand a little bit about information security threats, but I have no problem with that since I get help from IT staff because they are helpful. I usually depend on IT staff regarding updating anti-virus or any data error that exists in the system."*	Lack of knowledge	Self-Efficacy
P11	*"I do receive the emails, but, usually, I do not read it in detail, just glance through because it is too long. If the email is important and related to my job, then I will read it."*	Difficulty of retrieving the email	Perceived barrier
P6	*"It is very difficult to read emails that contain long information."*	Difficulty to read the email	Perceived barrier
P2	*"I believe that the ITD staff will take care of any security threat problem, so I do not bother about the security threats as long as I do my work well."*	Trust with IT staff	Trust
P5	*"If this policy was written and implemented by MOH, so then we have no query, we must follow the policies."*	Trust with the management	Trust
P1	*"I have no problem complying with the policies because I believe that these policies were implemented by the government and that it is important for us*	Confidence with the ISPs	Trust

	to comply with them."		
P1	*"I believe that information security threats are serious, so I ensure that I take care of the data as required in the policies."*	Seriousness of security threat	Perceived severity
P6	*"It is important for us to think about the consequences of not complying with the policies as our job is processing patients' data and this data is very confidential. If anything happens to the data, it might harm the patient and records' procedure."*	Harm the reputation	Perceived severity
P8	*"I do not want to be blamed because of my wrongdoing, so I will make sure that I do my job well."*	Blamed	Perceived severity
P11	*"I will not simply share hospital data with unauthorised users. I believe that patients' data is confidential and should be protected to avoid any serious problems. We might get a serious penalty if the data are lost or harmed."*	Serious problem	Perceived severity
P15	*"ISPs are important and should be implemented in the hospital because hospital data are confidential. The ISPs provide a guideline to users of how to*	ISPs benefit	Perceived benefit

	protect health data."		
P9	*"The anti-virus software installed in my computer is good and is able to prevent a virus being spread."*	Anti-virus benefit	Perceived benefit
P11	*"In this hospital, we cannot simply access the patient data, the system* (HIS) *recognises the level of authority before allowing a person access into the system based on the password used. So, I think this can reduce security risk*."	Security tool benefit	Perceived benefit
P14	*"The probability of information security threats existing is high, especially when all the health data are accessible through the online system; if we are not careful enough, like we do not log out from the system after use, other people will access it and look for information".*	Probability of existing	Perceived susceptibility
P17	*"Information security is very important for all hospitals that implement HIS, because this system allows confidential health data to be accessed online. Moreover, the possibility of the data being leaked through the online system is high, therefore I feel that it is necessary to have an information security system, and, as a*	Possibility of data leaking	Perceived susceptibility

	user, we are responsible for practising security behaviour properly."		

DISCUSSION

Based on the qualitative findings, the hospital management play their role in distributing the HIS security policies document implemented by Ministry of Health (MOH). The security policies are distributed via email and uploaded to the hospital server, whereby HIS users can download the security policies document from the hospital e-portal. However, a number of participants reported that they are concerned about how HIS security policies are conveyed to all employees in the hospital. The participants also argued that even though they have received the ISPs from their Head of Department (HOD), the content of the ISPs document was too long and difficult to read, which makes them unmotivated to read the policies. If employees are not motivated to read the policies and do not understand the policies very well, it might lead to ignorant behaviour and protection of the information security might fail (Johnston & Warkentin, 2008).

HODs should practice positive security behaviour and always remind all their staff in the department about practicing good security behaviour during meetings. Moreover, every HOD must ensure that all the policies and procedures related to HIS use are put into practice by all employees under their department as this can maintain the effectiveness of ISPs. Employees need to perceive that ISPs compliance is important to management. In doing this, hospital management should monitor and control employees' security behaviour and needs to indicate that the management view compliance with the policy as mandatory. In addition, the communication between leaders and their followers must also be effective. Therefore, IT management in public hospitals must provide different channels of communication for increasing the effectiveness of HIS security policies implementation, and, hence, increase HIS security protection. The proposed prototype is one method to improve the communication between the leaders and all the employees in the hospital. Through the prototype system, IT administrators are able to manage and monitor the process of distributing information security announcements to all employees in the hospital who have HIS access.

HIS training was shown to be an effective method to distribute the security message. Moreover, the training can help users to develop an understanding about ISPs. HIS users have different levels of education and knowledge, thus, the hospital management are responsible for training users accordingly. The ongoing training can also help to increase users' knowledge and awareness, thus improving security behaviour among employees. The qualitative findings of the current study indicated that users' awareness of the severity of information security threats (Perceived Severity) plays an important role in users' compliance with ISPs. The participants argued that the reason that they comply with hospital ISPs is to avoid any disciplinary action that may affect their career. Moreover, users' awareness about the susceptibility of information security threats (Perceived Susceptibility) also helps them to be more careful when handling health data when using HIS. The findings indicate that the participants who are not experienced with information security threats, do not consider that the likelihood of the occurrence of information security is high, which causes ignorant behaviour.

Moreover, this study also found that HIS users are aware of the benefit of security-countermeasures. They realise the importance of updating user passwords and scanning any portable device before connecting it to the computer. Therefore, it is very important to educate employees about the importance of practicing information security behaviour and follow all the rules and regulations related to HIS security adequately. The ISPs should be effectively documented and distributed to all employees in the hospitals. Additionally, in order for employees to feel confident in the security guidelines, so that they are able to practice it as recommended by the MOH, the ISP documents must be easy to understand and presented in simple language either distributed via email or through the online announcement messages developed in the prototype.

Additionally, most of the respondents believed that the proposed prototype would increase their level of trust in a positive way. Therefore, the HIS prototype can be a platform to distribute ISPs document or anything related with HIS security. However, the most concern is the writing style of the ISPs document, whereby it should be more attractive, if distributed thru HIS. This study suggested that the content style of ISPs should be further investigated in future study.

CONCLUSION

The interview data analysis through prototype testing revealed that HIS notification prototype that developed based on the following factors: Management Support and Information Security Awareness, contributes on improving user's compliance behaviour towards ISPs related with HIS uses. Moreover, the prototype able to alert users regarding to the new security policies, information security programmes and information security threats in more systematic way. This study believes that the research findings can contribute to human behaviour in information system studies and are particularly beneficial to policy makers in improving organizations' strategic plans in information security by emphasizing management and human-technical factor issues, especially in healthcare sectors. Most organizations spend time and resources to provide and establish strategic plans of information security; however, if employees are not willing to comply and practice information security behaviour appropriately, then these efforts are in vain. Thus, the HIS notification prototype will gives benefits to the organizations in implementing and distributing ISPs more effectively and efficiently.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the help of Universiti Teknologi MARA (UiTM) in providing the research fund for the project number: 600-IRMI/MYRA 5/3/LESTARI (0107/2016) and Faculty of Business and Management, UiTM Puncak Alam Campus for supporting the research work.

REFERENCES

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, In Computers & Security, 68, 145-159.

Bélanger, F., Collignon, S., Enget, K., Negangard, E. (2017). Determinants of early conformance with information security policies, In Information & Management, 54(7), 887-901.

Brady, J. W. (2011, 4-7 Jan. 2011). Securing Health Care: Assessing Factors That Affect HIPAA Security Compliance in Academic Medical Centers. Paper presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference.

Guo, K. H. (2012). Security-related behavior in using information systems in the workplace: A review and synthesis. Computers & Security, 3 (1), 242-251.

Höne, K., & Eloff, J. H. P. (2002). What Makes an Effective Information Security Policy?. Network Security, 2002(6), 14-16.

Johnston, A. C., & Warkentin, M. (2008). Information privacy compliance in the healthcare industry. Information Management & Computer Security, 16(1), 5-19.

Ng, B.-Y., Atreyi, K., & Yunjie, X. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. Computers & Security, 31(5), 673-680.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42(0), 165-176.

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, 43(0), 90-110.

Waly, N., Tassabehji, R., & Kamala, M. (2012, 25-27 June 2012). Improving Organisational Information Security Management: The Impact of Training and Awareness. Paper presented at the High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS).