2012 2nd International Conference on Management and Artificial Intelligence
IPEDR Vol.35 (2012) © (2012) IACSIT Press, Singapore

The Influence of Security Awareness and Security Technology on Users' Behavior towards the Implementation of Health Information System: A Conceptual Framework

Norshima Humaidi[1+] and Vimala Balakrishnan[2]

[1]Centre of Applied Management, Faculty of Business & Management, Universiti Teknologi MARA, 40150, Shah Alam, Malaysia.

[1]Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia.

[2]Department of Information Systems, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia.

Abstract. Implementation of health information system in health institutions provides many benefits to the organization. However, issues of information system security must be taken seriously as health records are strictly confidential and need to be protected as it might be exposed to unauthorized users. Users' behavior is known as one of information security issues that should be considered by organizations as they are encouraged to practice recommended information security behavior. This study aims to assess the influence of security awareness and security technology on users' behavior with regards to health information systems' security. This paper proposed and discusses the research framework which was developed based on Protection Motivation Theory and Health Belief Model. The current study will employ both quantitative and qualitative methods, specifically interviews and questionnaire surveys. As security aspect is an important element in information system, therefore, users' behavior should seriously be considered as a substantial issue that need to put forward.

Keywords: Health Information System, Security Awareness, Security Technology, Users' Behavior

1. Introduction

Information & Communication Technology (ICT) have been introduced in Malaysia for many years since 1990s. The rapid growth of ICT resulted in the Ministry of Health to introduce Health Information System (HIS) in several local hospitals such as Hospital Selayang and Hospital Kebangsaan Malaysia Medical Centre (UKMMC) [1]. HIS is defined as an integration of several systems designed to manage administrative, financial and clinical aspects of hospitals and developed to provide the best services to patients. However, the system is vulnerable to inappropriate use, both within, and without the medical institution that provide the care. Therefore, information security is required to protect health data from being stolen or harmed. Information security is defined as the protection of information systems from unauthorized access and information threat [2].

One of the major issues in HIS is human error. Previous studies agreed that human who are also users of the system are the weakest link in the information security chain [4 - 5]. Boujettif [3] stated that 80% of major security failures are due to the poor security behavior of the end-users who are also their internal employees. Even-though organizations have invested huge amount of money in security technology, yet user's behavior towards information security is still weak. The effectiveness of information security can be improved if user practices recommended security behavior. Therefore, the aim of this study is to propose a

+ Corresponding author. Tel.: +60196421428; fax: +6033258500.
E-mail address: [1]norshima24@yahoo.com. [2] vimala.balakrishnan@um.edu.my

research framework by taking security awareness and security technology into consideration. The study focuses on three main research questions, that is, 1) Does security awareness influence user's behavior towards information security 3) Does security technology influence user's behavior towards information security 4) Does users' behavior influence the effectiveness of health information system's security.

2. Conceptual Background

Theoretical framework in current study is conceptualized by Protection Motivation Theory (PMT) and Health Belief Model (HBM) because these two theories have been widely used in human behavior studies that are significant in predicting human behavior. Other critical factors believed to influence users' behavior towards information security are also included.

2.1. Protection Motivation Theory

PMT refers to "how people change their health attitude and behaviors in response to health risk message". The theory explains that if threat can be perceived by people as fearful, they will be more cautious and prevent the possible threat. PMT was applied successfully in many domains such as cancer [6] online harassment behavior [7]. These studies found that most of the factors, such as perceived severity and self-efficacy significantly influenced users to practice security behavior. PMT is based on four factors that are believed to motivate users to protect themselves, i.e., perceived severity, perceived vulnerability, perceived benefits and self efficacy. These factors are divided into two categories: threat appraisal (perceived severity and perceived vulnerability) and coping appraisal (perceived benefits and self efficacy). Threat appraisal states that if people have strong perception on the severity and vulnerability of a threat, it can motivate them to avoid security incidents [8]. Meanwhile, coping appraisal refers to the ability of people to avoid security risk and belief that they can practice recommended security behavior successfully.

2.2. Health Belief Model

Health Belief Model (HBM) explains and predicts preventative healthy behaviors widely used in health behavior studies such as drug [9] and cancer [10], among others. HBM predicts that if people understands certain illnesses and know how to prevent it, they are more cautious and will practice security behavior [10]. HBM suggests individuals determine the feasibility, benefits and cost related to an intervention or behavior change based on the following constructs: perceived susceptibility (similar to perceived vulnerability), perceived benefits, perceived barriers, cues to action, self-efficacy and perceived severity. Majority of previous studies indicated that most of the constructs influence human behavior. Therefore, this study adapts HBM to investigate the indicated factors influence on users' behavior on information security.

3. Research Framework and Hypotheses

As shown in Fig. 1, the study has two independent variables (security awareness and security technology), one mediating variable (Users' behavior towards information security) and HISSE as the dependent variable.

Security awareness refers to users' understanding towards the importance of information security and their responsibility to practice recommended information security behavior to protect organization's data [11]. The rapid rise of threats from viruses, worms and the likes has illustrated the need for increased awareness among users. Many previous studies found that employees have low user awareness and understanding of information security [4, 13].

Security technology refers to the technology used to protect information system such as firewall and user's authentication. Passwords are generally used to authenticate users, however, the method is considered weak due to users' behavior [14]. Security measures taken to strengthen password is not practiced by many users [15], whereby they are still unaware on the importance of choosing strong passwords and omit to change them regularly. Most of employees feel that security technology slows down their work and can be a rather tedious process as well [16]. Therefore, they usually omit to comply with the information security policies and as a result increase the vulnerability of the organization's data.

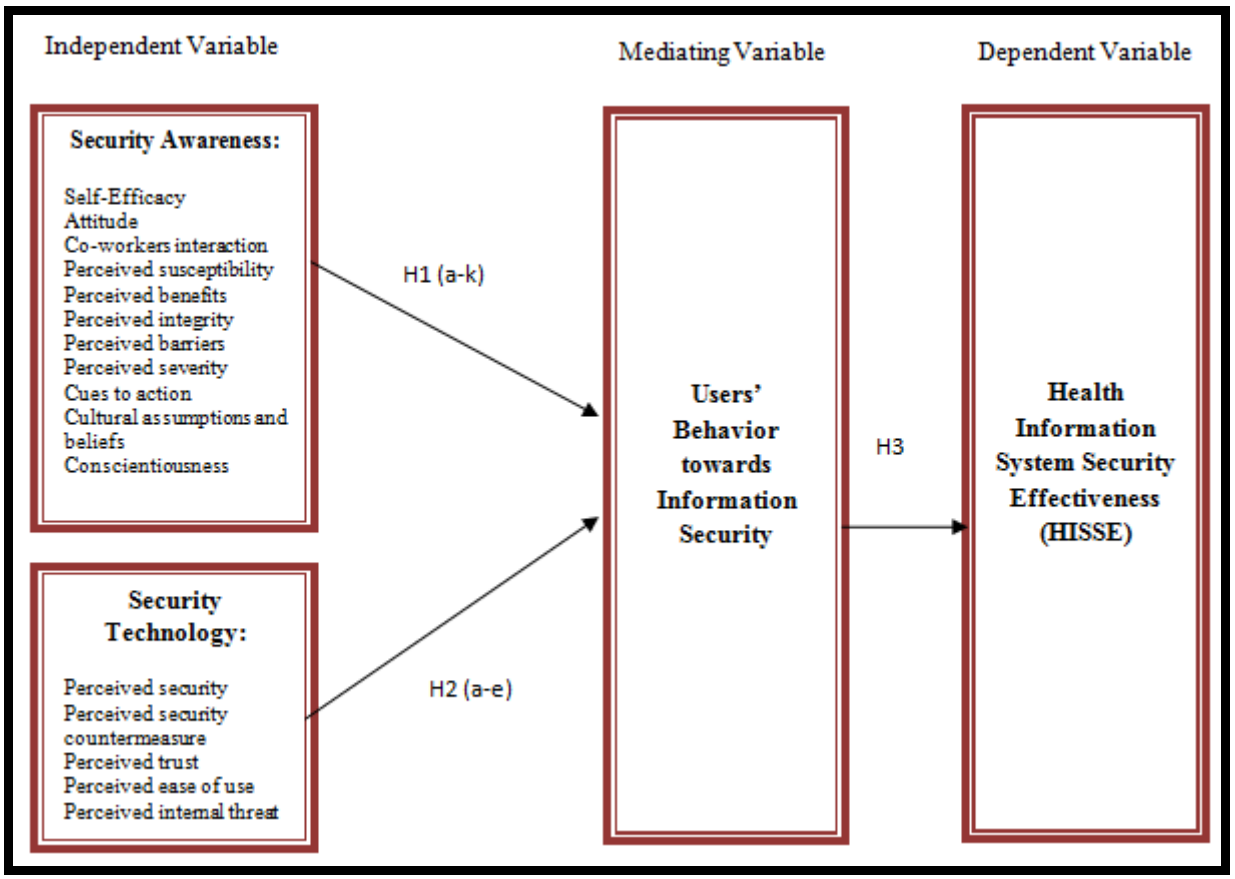

Fig. 1: Research framework

Table 1 described each of the constructs and defines all the related variables and hypotheses for this study.

Constructs	Operational Definitions/Hypotheses	Ref. of Authors
Security awareness:	Users' understanding towards the importance of information security and their responsibility to practice it to protect organization data.	[11]
▪ **Self-Efficacy**	Determine how people think, feel and motivate themselves to behave in a certain way based on cognitive, motivational, affective, social influences, and selection process. **H1(a): Self-Efficacy influences users' behavior towards information security.**	[16]
▪ **Co-Workers interaction**	Colleague's behavior which influences user's behavior. **H1(b): Co-workers interaction influences users' behavior towards information security.**	[17]
▪ **Perceived Susceptibility**	People belief on risk which can result seriousness of the condition. **H1(c): Perceived susceptibility influences users' behavior towards information security.**	[18]
▪ **Perceived benefits**	To what the person perceives as the positive outcomes of performing a certain health behavior. **H1(d): Perceived benefits influence users' behavior towards information security.**	[18]
▪ **Perceived Risk**	A combination of uncertainty plus seriousness of outcome involved. **H1(e): Perceived risk influence users' behavior towards information security**	[19]
▪ **Perceived Integrity**	Perception on ethical values and principles.	Self definition.

▪ **Perceived Barriers**	**H1(f): Perceived integrity influence users' behavior on information security.**	
▪ **Perceived Severity**	User's perceptions towards the difficulty of practicing computer security, which is likely to reduce the performance of computer security behavior. **H1(g): Perceived barriers influence users' behavior towards information security.**	[18]
▪ **Cues to Action**	User's perceived seriousness of a security incident, which should lead to greater computer security behavior. **H1(h): Perceived severity of security incidents influence user's behavior towards information security.**	[18]
▪ **Cultural Assumptions and Belief**	Users' experience on security threat which can encourage and activate them to practice computer security. **H1(i): Cues to action influence users' behavior towards information security.**	[20]
▪ **Conscientiousness**	People's think which can motivate them to do things or actions. **H1(j): User assumptions and belief influences users' behavior towards information security**	Self definition.
	A trait that reflects individuals' extent of determination, will, and violation. **H1(k): Conscientiousness influences users' behavior towards information security**	[21]
Security technology:	Technology used to protect information system such as firewall, user's authentication, encryption and etc.	Self definition
▪ **Perceived security**	Users' ability to protect data against unauthorized access. **H2(a): Perceived security influence users' behavior towards information security.**	[22]
▪ **Perceived security countermeasure**	Method to detects, prevent or minimize risks that related with information system threat. ***H2(b): Perceived security countermeasure influence users' behavior towards information security***	[23]
▪ **Perceived trust**	Users feel on security and their willingness to adopt it. ***H2(c): Perceived trust influences users' behavior towards information security***	[24]
▪ **Perceived ease of use**	Easy to understand by user, easily to be adopted and definitely not too strict will encourages user to behave appropriately on information security. ***H2(d): Perceived usefulness of security influences users' behavior towards information security***	Self definition
▪ **Perceived internal threat**	Threat by insiders (employee, ex-employee, partner or client) who misuse the access given by the organization in a negative way which give an impact to the effectiveness of information system security. ***H2(e): Perceived internal threat influences users' behavior towards information security***	[5]

4. User's Behavior and Information Security System Effectiveness

Many literatures agreed that the effectiveness of information system security depends on users' behavior [4, 25]. Koskosas et al. [12] stated that employees must be proactive on information security. If the whole organization practices recommended information security, the level of user awareness can be increased and this gives an impact to the success of the implementation of information system's security in the organization. This is especially true in medical domain as health information is sensitive and requires high confidentiality. Information system's security effectiveness is defined as the ability of information system security measures to protect against the unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against hardware, software and data [4]. The study believes that if users' behavior towards information security is acceptable, security incidents can be decreased, and effectiveness of information system's security can be increased.

H3: Acceptable users' behavior on information security will increase the effectiveness of Health information Security System.

5. Research Methodology

Current study comprises both quantitative and qualitative methodologies, which include interviews and questionnaires surveys. The target population of this study will be health care professionals (nurses, physicians, radiologist, pharmacists, laboratory technicians and radiographers) in government hospitals, Malaysia. In Malaysia, there are about 134 government hospitals. However, to obtain the required sample size, only two hospitals at each region (northern, southern, East Coast, Central) and one hospital in Sabah, Sarawak and Labuan will be selected. Target sample size is 500 respondents and will be selected using stratified random sampling by region.

6. Conclusion

Health information system provides many benefits to health institutions as patients' health records and administrative works can be managed effectively and efficiently. The system enables information sharing among related healthcare providers. However, with this development, health institutions face new challenges due to security problems, most of which related to user's behavior. Therefore, it is important to investigate the critical factors that influence users' behavior towards information security. The study focused on two variables: security awareness and security technology. The conceptual framework was developed based on Protection Motivation Theory and Health Belief Model. The framework will be used for future work to investigate the factors that influence users' behavior towards information security. The results of the study will help to identify new requirements for information system's security and able to overcome current issues of information system's security in the organizations.

7. References

[1] A. Ismail*, et al.*, "The implementation of Hospital Information System (HIS) in Tertiary hospitals in Malaysia: A qualitative study," *Malaysian Journal of Public Health Medicine* vol. 10, pp. 16-24, 2010.

[2] E. Cavalli*, et al.*, "Information security concepts and practices: The case of a provincial multi-specialty hospital," *International Journal of Medical Informatics,* pp. 297-303, 2004.

[3] M. Boujettif and W. Yongge, "Constructivist Approach to Information Security Awareness in the Middle East," in Broadban*d, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on*, 2010, pp. 192-199.

[4] J. W. Brady, "Securing Health Care: Assessing Factors That Affect HIPAA Security Compliance in Academic Medical Centers," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, 2011, pp. 1-10.

[5] L. Kreicberge, "Internal threat to information security - countermeasures and human factor with SME," Master Thesis, Continuation Courses Security Master, Business Aministration and Social Sciences, University of Technology, 2010.

[6] D. N. Cox*, et al.*, "Predicting intentions to consume fucntional foods and supplements to offset memory loss using an adaption of protection motivation theory," *Appetite,* vol. 0, pp. 55-64, 2004.

[7] M. O. Lwin*, et al.*, "Stop bugging me: An examination of adolescents' protection behavior against online harassment," *Journal of Adolescence,* 2011.

[8] L. Younghwa, "Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective," *Decision Support Systems,* vol. 50, pp. 361-369, 2011.

[9] E. E. Bonar and H. Rosenberg, "Using the health belief model to predict injecting drug users' intentions to employ harm reduction strategies," *Addictive Behaviors,* vol. 36, pp. 1038-1044, 2011.

[10] C. L. Bylund*, et al.*, "Using the Extended Health Belief Model to understand siblings' perceptions of risk for hereditary hemochromatosis," *Patient Education and Counseling,* vol. 82, pp. 36-41, 2011.

[11] R. S. Shaw*, et al.*, "The impact of information richness on information security awareness training effectiveness," *Computer & Education,* vol. 52, pp. 92-100, 2009.

[12] I. Koskosas, *et al.*, "Examining the linkage between information security and end-user trust," *International Journal of Computer Science & Information Security,* vol. 9, pp. 21-31, 2011.

[13] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Computers & Security,* vol. 29, pp. 196-207, 2010.

[14] K.-P. L. Vu, *et al.*, "Improving password security and memorability to protect personal and organizational information," *International Journal of Human-Computer Studies,* vol. 65, pp. 744-757, 2007.

[15] A. Srivastava, "Electronic signatures and security issues: An empirical study," *Computer Law & Security Review,* vol. 66, pp. 45-56, 2009.

[16] M. Workman, *et al.*, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior,* vol. 24, pp. 2799-2816, 2008.

[17] W. Ping An, "Information security knowledge and behavior: An adapted model of technology acceptance," in *Education Technology and Computer (ICETC), 2010 2nd International Conference on*, 2010, pp. V2-364-V2-367.

[18] B.-Y. Ng, *et al.*, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems,* vol. 46, pp. 815-825, 2009.

[19] J. M. O. Egea and M. V. R. Gonzalez, "Explaining physicians' acceptance of EHCR systems: an extension of TAM with trust and risk factors," *Computers in Human Behavior,* vol. 27, pp. 319-332, 2011.

[20] M. Siponen, *et al.*, "Compliance with Information Security Policies: An Empirical Investigation," *Computer,* vol. 43, pp. 64-71, 2010.

[21] G. Bansal, *et al.*, "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems,* vol. 49, pp. 138-150, 2010.

[22] S. Dong-Hee, "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption," *Interacting with Computers,* vol. 22, pp. 428-438, 2010.

[23] Q.-J. Yeh and A. J.-T. Chang, "Threats and countermeasures for information system security: A cross-industry study," *Information & Management,* vol. 44, pp. 480-491, 2007.

[24] M.-J. Kim, *et al.*, "The effect of perceived trust on electronic commerce: shopping online for tourism products and services in south Korea," *Tourism Management,* vol. 32, pp. 256-265, 2011.

[25] S. Moller, *et al.*, "Modeling the behavior of users who are confronted with security mechanisms," *Computer & Security,* vol. 30, pp. 242-256, 2011.