Australian Journal of Basic and Applied Sciences, 5(9): 291-297, 2011
ISSN 1991-8178

Investigating the Relationship of Users' Behavior and Internal Security Threat towards the Implementation of Total Health Information System (THIS) in Malaysian Medical Institutions

[1]Norshima Humaidi, [2]Noor Azzah Said and [3]Norzaidi Mohd Daud

[1]Faculty of Office Management and Technology, Universiti Teknologi MARA 42300 Kampus Puncak Alam Selangor, Malaysia/Universiti Malaya
[2]Faculty of Office Management and Technology, Universiti Teknologi MARA 42300 Kampus Puncak Alam Selangor, Malaysia
[3]Faculty of Business Management/Accounting Research Institute/Institute of Business Excellence Visiting Professor, King Saud, University, Saudi Arabia

Abstract: This paper have been carried out with the purpose to develop research model that can be used to investigate the relationship of users' behavior and internal security threat towards the implementation of Total Health Information System (THIS). In doing so, several study related with health information system and information security effectiveness have been reviewed to construct research model. The study only focuses on medical institution which fully implements THIS. The outcome of the study will help the researcher to conducts study regarding information security management which significant to the medical institution in improving health record management. Security aspect is an important in medical institution which implements THIS. However, without good management practice this cannot be implemented effectively and efficiently. The study is perhaps one of the first to develop THIS performance model to investigate the relationship of users' behavior and internal security threat.

Key words: Total Health Information System, THIS, Information Security, Users Behavior, Internal Security Threat

INTRODUCTION

Medical institutions are realized that developing information system that use to store health information is vital however such the new development of patients records transferred through Internet have produced significant difficulties for patients (Farzandipour et. al, 2009) as security defect in its system can disclose hundreds or thousands records (Aspen Reference Group, 1999).

Health Information System required three aspects of security, which are confidentiality, integrity and availability (CIA) (Haas *et al*., 2010). Hass *et al*. also stated that the system required strong confidentiality as the health information is an important in medical. Integrity is essential since in correct treatment based on erroneous medical data might be total. Moreover, availability is also as important as integrity because the information in health information system might be necessary for adequate treatment.

To protect patient medical information is a critical issue (Anderson, 2000). Problem can be arising if patient medical information can be accessed through Internet or the use of secondary storage by non-healthcare providers. Those data will be used by third party payers to process claims and to manage pharmacy benefits programs (Anderson, 2000). Moreover, Bansal *et al*. (2010) claimed that disclosure of personal health information may result in discrimination by employers insurance agencies if they get access to such information and could manipulate the information in the systems. The systems provide more cost effective health care and to support the information needs of integrated delivery systems. However, these systems are vulnerable to inappropriate use, both within, and without the medical institution that provide care (Anderson, 2000). Anderson also stated that "*the systematic use of patient-identifiable health information by insurers, employers, drug companies, and commercial marketing firms poses major threats to the privacy and security of health information"* (p.116).

Corresponding Author: Norzaidi Mohd Daud, Faculty of Office Management and Technology, Universiti Teknologi MARA 42300 Kampus Puncak Alam Selangor, Malaysia/Universiti Malaya
E-mail: zaidiuitm2000@yahoo.com

Hackers are also one of health information security threat as hackers could access health information if the provider lacks adequate data security. Threats to information security have been study for many years ago. Most of the studies examined in related fields were categorized as studies of computer abuse or computer ethics (Whitman, 2004). He also stated that viruses, worms, hackers, and employee abuse and misuse have created a dramatic need for understanding and implementing quality information security. Many organizations suspect that their internal security threat is more pressing than their external security threat (Leach, 2003). Leach stated that internal threat is predominantly the result of poor user security behavior. Study found that user unfamiliar with possible threats and failed to recognize the value of their information security role in the organization (Albrechtsen and Hovden, 2009). This issue can become a problem and jeopardize the organization and especially when it deals with patient medical information.

In Malaysia, the most critical threat for health information system is power failure followed by acts of human error and other technological factors (G. Narayana *et al*., 2010). Stated by Verizon (2009), staff in the organization could be behind most security breaches, whether intentionally or unintentionally. Staff or prefer known as insiders may pose a threat to the protection of information (Andric *et al*., 2010). According to Schneier (2000) users are often the weakest link in the information security chain, as users might be a single or the least reliable barrier to prevent unwanted incidents.

Very few study have investigates on the relationship of users' behavior and internal security threat. Janczewski and Shi (2002) stated that the major security weakness of mot health information system is not technology but the people involved. His research also indicated that 50% of security threat was internal security attack. Therefore, this study is concentrates on the issue of internal security threat because it is important to determine the system security performance. Besides, it is also important to understand factors that influence users' behavior on information security. Hence, the study have construct research model that can be investigated the relationship of users' behavior and internal security threat towards the implementation of Total Health Information System (THIS) in medical institution. The next section presents the literature and propositions that are formulated and tested in this study.

Literature Review:

Electronic Health Record:

Many medical institutions are now moving forward with the new system development to store medical information. Electronic health record or also called as health information system is develop for the purpose to provide a documented record of care which supports present and future care by the same or other clinicians (ISO/TS 18308). This documentation provides a means of communication among clinicians contributing to the patient's care (Linden *et al*., 2009). Other researcher defined electronic health record as repository of information regarding the health status of a subject of care in computer processable form, stored and transmitted securely, and accessible by multiple authorized users (Kalra *et al*., 2009). Its primary purpose is the support of continuing, efficient, and quality integrated health care and it contains information which is retrospective, concurrent and prospective. End-user of health information system is user needs access to the information to provide adequate care to the patient.

Information Security:

Information security information security is classically defined as the preservation of confidentiality, integrity and availability (Cavalli *et al*., 2004). Information is important and is depicted as the lifeblood of the growing electronic economy (Gordon, 2002). Same goes to protecting other people information especially when it is relate with health information. Health information is confidential and users need to protect owners' privacy. Information need to be protected when it's to be transmitted, stored and processed (Dlamini *et al*., 2009). In Health Organization, patients' health records are distributed around different hospitals and clinics, and the retrieval of this scattered information when a patient visits a doctor in any particular hospital is a major problem (Huang *et al*., 2009). Therefore, the security information needs to be managed and controlled properly. Information Security (IS) has evolved from addressing minor and harmless security breaches to managing those with a huge impact on organizational economic growth and important in organization and particularly where personal and medical information is routinely recorded (Dlamini *et al*, 2009).

Also, Rezgui *et al*. (2008) stated that Information System security is strongly related to the concept of risk. The International Organization of Standardization (ISO) defines risks as the potential that a given threat will exploit vulnerabilities of an asset or groups of assets. Moreover, they found that the impact of relative severity of the risk is proportional to the business value of the loss or damage and to estimates frequency of threat. IS may include protection of resources, maintaining management control, ensuring safety and integrity,

implementing policies and laws, and attaining operational advantages and economies. They also stated that an educated security attitude of employees, management, and external IT users and partners is also vital to ensure effective IS. Other elements that should be considered are security awareness and education, clear organizational culture and incident handling and response that can deliver a clear picture of where IS a stand within organizations.

Conceptual Background:

To develop conceptual framework, several studies regarding to IS and factors influence users' behavior on IS have been reviewed. Based on the finding, researcher have decided to use security awareness which includes self-efficacy, attitude, perceived susceptibility, social environment, cultural assumptions and beliefs, and conscientiousness as independent variable. Perceived severity will taken as moderator variable. In this research, users' behavior on IS will be taken as mediating variable which is believe can influence to effectiveness of THIS.

Is Security Awareness:

IS security awareness means as user's attention to IS security issues, or users' understanding of IS security and optimally committing to it (Rezgui *et al*., 2008). There is an obvious need for increased awareness of the threats to IS not only among security and system administrators, but also among the users of information in organizations. They also stated that the role of users enhancing the IS security culture. The rapid rise of threats from viruses, worms and the like has illustrated the need for increased awareness by users. Even though the organizations have good security policy, but still ineffective if not implemented and enforced to among users of information (Whitman, 2004).

Self-Efficacy:

Self-efficacy is a person's self-confidence in his ability to perform a behavior and the roots of self-efficacy theory and it is refers to an individual's self-confidence in his ability to perform a behavior (Ng *et al*, 2009). According to social cognitive theory, individuals with greater confidence in their abilities are more likely to initiate challenging behaviors (Rimal, 2000). This support by Rhee *et al*. (2009), people with a high level of self-efficacy have a stronger form of self conviction about their ability to mobilize motivation, cognitive resources, and course of action needed to successfully execute a task. Moreover, they believed that self-efficacy influences the amount of effort, self regulation, and the initiation and persistence of coping efforts in the face of obstacles. The role of self-efficacy on user behavior can control over potentially threatening events and people with high self-efficacy are likely focusing their attention on analyzing and formulating solutions to problems. Meanwhile, people with low self-efficacy tend to engage in fewer coping efforts. As a conclusion, based on the previous research, researcher believe that factor of self-efficacy can influence users' behavior on IS. People with self-efficacy are believes to follow recommended security conscious behavior in order to protect information.

H1 (a): Self-Efficacy Influences Users' Behavior on Information Security.

Attitude:

People attitude are an important factor that influence users' behavior towards IS. This is because attitude is one of the elements in IS security awareness that use to interact with the organization's systems and procedures at any point in time. In the end-user support context, attitude can be defined as the user's evaluative judgment of the support source (Govindarajulu *et al*., 1999). The attitude can be positive or negative, depending upon evaluation of the support source. If people have positive attitude, researcher believe that the information security system can be strong and vice versa. Especially in medical institution, employee who responsible in medical information must have positive attitude as medical information is needs strong confidentiality. In this study, attitude is the determinant of a users' behavior on IS.

H1 (b): User Attitude Influences Users' Behavior on Information Security.

Perceived Susceptibility:

Perceived susceptibility is taken from health belief model. This construct refers to the subjective risks of contracting condition (Ng et al, 2009). Furthermore, perceived susceptibility also refers to a user's perceived probability of a security accident happened and jeopardized the organization. Researcher believes that if users more concern about the security accident risk, they will securely behave.

H1 I: Perceived Susceptibility to Security Incidents Is Related to Users' Behavior on Information Security.
Social Environment:

Social environment in this contacts is focus on the behavior demonstrated by others will influences user attitudes. Leach (2003) stated that the company's body of knowledge will be undermined if its stated principles, policies and procedures are contradicted by the practices that people see in evidence around them. What people are shown needs to support rather than contradict what they are told. Furthermore, medical institution must ensure that its principles and policies are followed by all senior management and junior staff. Hence, good information security management can be implemented effectively and efficiently.

H1 (d): The Social Environment Influences Users' Behavior on Information Security.
Cultural Assumptions and Beliefs:

Cultural assumptions and believe by user may influence their behavior at work (Veiga and Eloff, 2010). People who are responsible in managing medical information should People who are responsible in managing medical information should have strong believes that medical information is confidential and they will follow right security policy. These people will be more cautious to avoid risks.

H1 (e): User Assumptions and Belief Influences Users' Behavior on Information Security.
Conscientiousness:

Conscientiousness is a trait that reflects individuals' extent of determination, will, and violation (Bansal *et al*., 2010). Other researcher has stated that conscientious individuals have more precautions and foresight (Chauvin *et al*., 2007). According to Bansal, these people are detail-oriented and action-oriented and undertake initiatives needed for successful completion of tasks. They are also less risk-oriented and less willing to get involved in unsafe situations (Paunonen and Ashton, 2001; Vollrath, Knoch and Cassano, 1999). Thus, users with high conscientiousness should be more acceptable behave on IS.

H1 (f): Conscientiousness Is Influences Users' Behavior on Information Security.
Perceived Severity:

Ng. *et al*. (2009) define "*perceived severity to be a user's perceived seriousness of a security incident, which should lead to greater computer security behavior*" (p.820). Users must seriously consider on computer security incident. If the organizational data is loss of confidentiality, integrity, or availability may give negative impact to the organization and disrupt employees' work. If users understand the consequences of not practices a good computer security behavior, they will lost job and damage organization's reputation, and this will help them more cautious on security accident and securely behave.

H2: Perceived Severity of Security Incidents Increased the Effect of User Security Awareness and Users' Behavior on Information Security.
Users' Role in Is and Internal Security Threat:

The information security function is an important part of information security (Albrechtsen, 2007). One of the failures to IS is users' behavior. If they did not properly behave and incautious on IS actions, this may jeopardize the organization value and profit. Therefore, the organization must pay attention on insider threat or internal security threat. Internal security threat is a threat are encompassing a broad range of events, incidents and attacks, all connected by being caused not by external people who have no right to be using the corporate IT facilities but by the organization's own staff, its authorized IT users (Leach, 2003). Study done by Colwill (2010) was highlights that awareness and mitigation of internal threat varies greatly among companies and sectors and is often dealt with poorly. In his research also concludes that in the UK many organizations are still not doing enough to protect themselves and their customers' information. This threat is cover user negligence and deliberate acts against the company. It encompasses behaviors such as a lack of security common sense, forget to apply security procedures and users taking an inappropriate risks because they did not appreciate or believe the level of risk involve and etc (Leach, 2003). Medical institution need to control and monitor their staff or employee behavior on information security. Information security role of users is an important part of a holistic approach to information security management (Albrechtsen, 2007).

H3: Users' Behavior on Information Security Influences Internal Security Threat.
H4: Internal Security Threat Influences the Performance of Total Health Information System.
Research Model:

Figure 1 depicts the model of THIS management performance proposed in this study. Research model was constructed based on previous researchers. Links among independent, moderating, mediating and dependent variables constitutes the hypotheses for this research.

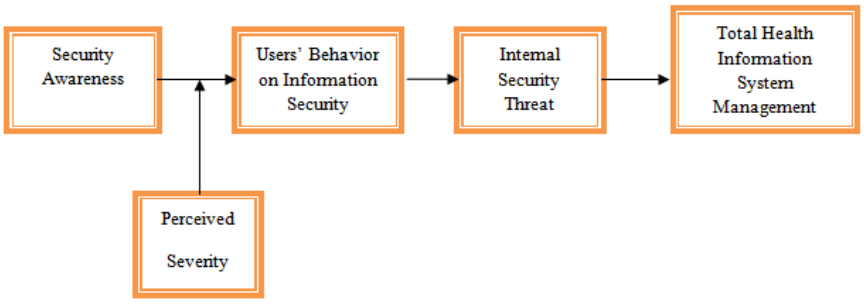

Fig. 1: Proposed of THIS model.

Conclusion:

Modern development in medicine, information technology and telecommunications are transforming healthcare, and support objectives of timely access to quality, cost effective healthcare for all people. Medical institution has begun to implement health information system which the system can manage and provide sharing information among related healthcare providers. Internets also have been used as a medium to distribute health-related information. However, with this development, medical institutions have faced new challenges to security problems. Most of the problems are come from internal threat. Medical Institutions are vulnerable to security attacks due to the fact that they contain sensitive information. This is serious when the institution implements information system, whereby, the information can be retrieved through online. If the employees disobey the information security policy will result serious jeopardy to the institution. Hence, the study have proposed Total Health Information System (THIS) model and hoped it can be used to investigate and dig out the influence of users' behavior and internal security threat towards the implementation of THIS in medical institution.

To manage medical records effectively and efficiently is important. This can be done by considering element of information security such IS awareness. To meet organization information security objective, one approach should be considered is information security management. As stated by Ashenden (2008), *"the management of information security depends on technology, processes and people"* (p.195). Organization must able to control how IS policies being implemented because the effectiveness of IS management system is directly divided by the effectiveness of the implemented IS control.

Medical institution must aware and seriously consider on information security issues especially internal security threat. Internal security threat is poses by employees in the organization. To manage people behavior is a challenge to organization. If the employees do careless, this will place Medical Institutions reputation in serious jeopardy (Siponen *et al*., 2009). Therefore, it is important to understand factors that may influences users' behavior on information security such as social environments, self-efficacy, attitude, and etc. By investigating these factors, researcher believes that it will help the organization especially medical institution to strengthen information security management by controlling internal security threat. Avoiding this problem will lead to information security incidents and failures that can cause losses of organization's revenue. It is important to increase IS vigilance because is good for medical institution reputation and increasing revenue.

The major threat to information security arises from careless employees. These types of employees sometime fail to comply with organization's information security policies and procedures (Siponen et. al, 2010). Therefore, increasing user security awareness and understanding towards information security system is necessary. Pattinson and Anderson (2007) stated that organization must pay attention on user awareness and behavior because both factors are actually as a central focus of an information security strategy. In addition, other researcher also stated that user security awareness is critical IS components (Da Veiga and Eloff, 2007). This is serious and management must take fully attention on this issue. Especially, medical institution is an organization which keeps patient information. Patient's information requires highly protection. Thus, implementation of information security system in medical institution is highly recommended to monitor and control.

As a conclusion, the proposed model will hope to help other researcher who is interested in the topic to investigate the relationship of users' behavior on information security and internal security threat towards the implementation of THIS. The model also can be applied for other industry that implements total information system in their business process. Other factors that might not list in this study also are recommended to investigate such as organization culture and top management support. The result of the study will hope to

improve the performance of information security in the organization and increasing the profits. The results of the study might help organization especially medical institution strengthen their information security system policy and able to avoid any condition that can cause problems to the organization. Thus, THIS model is highly recommending be testing, analyzing and evaluating.

ACKNOWLEDGMENT

Praise to The Almighty Allah for giving us the time, strength and patience in completing this study. Our thanks and appreciation goes to whom that had contributed to this study by spending their precious time to share their knowledge and ideas. Without their cooperation, we would not be able to complete the concept paper.

REFERENCES

Albrechtsen, E., J. Hovden, 2009. The information security digital divide between information security manager and users. Computers & Security, 28: 476-490.

Albrechtsen, E., 2007. A qualitive study of users' view on information security. Comp. and Sec., 26: 276-289.

Anderson, G.J., 2000. Security of the distributed electronic ptient record: a case-based approach to identifying policy issues. Inter'l J. of Med. Inform., 60: 111-118

Ashenden, D., 2008. Information Security management: A human challenge?.Information Security Technical Report, 13: 195-201.

Aspen Reference Group, 1999. Health information management manual. 1st ed. Aspen: Maryland, 51.

Bansal, G., F.M. Zahedi and D. Gefen, 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Dec. Supp.Sys., 49: 138-150.

Cavalli, E., A. Mattasoglio, F. Pinciroli and P. Spaggiori, 2004. Information Security concepts and Practices: The case of a provincial multi-specialty hospital. Inter'l J. of Med. Inform., 297-203.

Chauvin, B., D. Hermand, D.E. Mullet, 2007. Risk perception and personality facets. Risk Analysis, 27(1): 171-185.

Colwill, C., 2010. Human factors in information security: The insider threat- Who can you turs these days? Inform. Sec. Tech. Rep, 14, 186-196.

Da Veiga, A. and J.H.P. Eloff, 2007. An information security governance framework. Information system Management, 24(4): 361-372.

Dlamini, M., J. Eloff and M. Eloff, 2009. Information security: The moving target. Comp.and Sec., 23(3): 189-198.

Farzandipour, M., F. Sadoughi, M. Ahmadi and I. Karimi, 2009. Security Requirements and Solutions in Electronic Health Records: Lessons Learned from a Comparative Study. Sp. J., DOI 10.1007/s10916-009-9276-7.

Narayana Samy, G. Rabiah Ahmad and Zuraini Ismail, 2010. Security Threats Categories in Healthcare Information Systems. Health Inform. J., 16(3): 201-209.

Gordon, G., 2002. Dozens of threats beset your data. Sunday Times, Business Surveys 2002, May 2; [online] [cited 17 July 2002]. Available from;http://www.suntimes.co.za/2002/05/12/business/surveys/internet/survey10.asp.

Govidarajulu, C., B.J. Reithel and V. Sethi, 1999. A model of end user attitudes and intentions toward alternative sources of support. Inform. and Mgt., 33(4): 77-86.

Hass, S., S. Wonlgemuth, I. Echizn, N. Sonehara, G. Muller, 2010. Aspects of privacy for HER. Int'nl J.of Med. Inform., 2(1): 34-38.

Huang, L.C., H.C. Chu, C.Y. Lien, C.H. Hsiao and T. Kao, 2009. Privacy preservation and information security protection for patients' portable electronic health records. Comp. in Bio. Med., 39: 743-750.

Jafari, S., F. Mtenzi, R. Fitzpatrick and B. O'shea, 2009. An approach for developing comparative security metrics for healthcare organization. IEEE Computer Society.

Janczewski, L., F.X. Shi, 2002. Development of information security baselines for healthcare information systems in New Zealand. Comp. and Sec., 21(2): 172-192.

Kankanhalli, A., H.H. Teo, B.C. Tan and K.K. Wei, 2003. An integrative study of information systems security effectiveness. Inter'l J. of Inform. Mgt., 23: 139-154.

Luck, J., C. Chang, E.R. Brown, J. Lumpkin, 2006. Using local health information to promote public health, Health Affairs, 25(4): 979-991.

Leach, J., 2003. Improving user security behavior. Comp. and Sec., 22(8): 34-44

Linden, H.V., D. Kalra, A. Hasman and J. Talmon, 2009. Inter-organizational future proof EHR systems: A review of the security and privacy related issues. Inter'l J. of Med. Inform., 78: 141-160.

Ng, Y.B., A. Kankanhalli and Y.C. Xu, 2008. Studying users' computer behavior: A health belief perspective. Dec. Supp. Syst., 46: 815-825.

Pattison, M.R. and G. Anderson, 2007. How well are information risks being communicated to your computer users?. Information Management & Computer Security, 15(5): 362-371.

Paunonen, S. and M. Ashton, 2001. Big five factors and facets and the prediction of behavior. J.of Personal.and Soc. Psycho., 81: 524-539.

Rezgui, Y. and A. Marks, 2008. Information security awareness in higher education: An exporatory study. Comp.and Sec., 27: 241-253.

Rhee, H.S., C. Kim and Y.U. Ryu, 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. Comp.and Sec., 28: 816-826.

Rimal, R.M., 2000. Closing the knowledge-behavior gap in health promotion: the mediating role of self-efficacy, Health Comm., 12(3): 22-34.

Russel, D. and G. Gangemi, 1991. Computer security basics. Unites States of America: O' Reilly and Associates, Inc.

Sekaran, Uma. Research Methods for Business: A skill-building approach, 4th edition, 2003. John Wiley and Sons

Schneier, B., 2000. Secrets & lies. Digital Security in a networked world. New York: John Willey.

Siponen, M., S. Pahnila, M. Adam Mahmood, 2010. Compliance with information security policies: An empirical investigation. IEEE Computer Society, 64-71.

Sword and Shield, 2001. Top 10 list of proactive security measures. Retrieved November 7, 2010, from Sword and Shield Security Consultans: http://www.sses.net/top10.html.

Thomson, K.L. and R.V. Solms, 2005. Information security obedience: a definition. Comp.and Sec., 69-75.

Veiga, A.D. and J. Eloff, 2009. A framework and assesment instrument for information security culture. Comp. and Sec., 29: 196-207.

Verizon, 2009. Data breach investigations report. Retrieved November 7, 2010, from Verizon Business: http://www.verizonbusiness.com/resources/security/reports/2009databreach rp.pdf;2009.

Vollrath, M., D. Knoch and L. Cassano, 1999. Personality, risky health behavior and perceived susceptibility to health risks. Risk and Journal of Personality, 13: 39-50.

Whitman, M.E., 2004. In defense of the realm: understanding the treat to information security. Inter'l J. of Infor. Mgt., 24: 43-57.