Australian Journal of Basic and Applied Sciences, 6(12): 226-233, 2012
ISSN 1991-8178

Security Effectiveness in Health Information System: Through Improving the Human Factors by Education and Training

[1]Ahmad Bakhtiyari Shahri, [2]Zuraini Ismail, [1]Nor Zairah AB.Rahim

[1]Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, 81310 Johor Bahru, Malaysia
[2]Advanced Informatics School (AIS), Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia

Abstract: Security in Health Information Systems (HIS) is a central concern of researchers, academicians, and practitioners. Increased numbers of data security breaches have caused concern over the humans' role as the different users in security of HIS. Since many human errors or failures in all information systems (IS) can be prevented with education and training, this study tries to investigate the effects of education and training on significant human factors in HIS security. This paper also proceeds in describing how the data was collected. Secondary data resources are used in highlighting the security culture and security awareness of users as the significant factors for the implementation of security effectiveness in the healthcare domain. The results from this research will also provide some guidance and insights to both researchers and professionals of information security in the health care domain.

Key words: health information system, education and training, security awareness, security culture

INTRODUCTION

Security in information systems depends on many factors and numerous technical advances such as using security application cannot always create a safe and secure environment alone (Kraemer *et al*., 2009). This is because; the key to achieving effectiveness security is through considering both technical and human dimensions. For example, based on the results of studies, security of human resources is one of the weaknesses of the electronic health systems in Iran (staff need security in job responsibilities, training, and report all of security incidents) (Farzandipour *et al*., 2010). Therefore, insider users by creating or preventing of various threats are considered as the biggest threat to the security of different IS (Ma *et al*., 2008, Williams, 2009, Parsons *et al*., 2010).

In addition, since computers in each environment are employed by human directly or indirectly, information security is known as human factor that influences the interaction between individuals and information security technology (Parsons *et al*., 2010). Some studies also confirm that many of the errors or failures in all information systems can be prevented by human factors such as security awareness and improving the security culture. That is the reason why many of the researchers believe that users are the significant security components in all ISs such as HIS (Ma *et al*., 2008, Williams, 2009, Parsons *et al*., 2010, Bakhtiyari Shahri and Ismail, 2012a).

Since a threat is any action posed by a human or non-human source and that can originate internally or externally (Narayana Samy *et al*., 2010) so, it can be defined as indication of anything destroyed or modified data and threatens the confidentiality, integrity, and availability of health information assets (Huang *et al*., 2010).

Managers in healthcare domains need to identify the threats to healthcare assets. Providing an up-to-date category of threats can help to highlight the role of human in different threats to HIS. Consequently, by understanding the threats and their sources to HIS security, the organization can provide the educational requirements and training guidelines for users to better protect HIS assets. Therefore, this study first identifies different threats to HIS and tries to find the place of human in them. After that, by conducting a literature review on the security culture and the security awareness the study shows the importance of these factors to threats to HIS security. Moreover, as education and training are the most effective countermeasures against the threats by human to information security; it can also contribute to an increase in the level of users' knowledge and a decrease potential risk by positive changes in users' behavior. Therefore, finally, the study climes that education and learning can be used to support these emerging factors that affect on the information security effectiveness in healthcare domains.

Corresponding Author: Ahmad Bakhtiyari Shahri, Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, 81310 Johor Bahru, Malaysia.
E-mail: bsahmad2@live.utm.my

Research Methodology:

This paper proceeds in describing how the data was collected. Secondary data resources assist in providing the relevance of humans' factors in security of HIS; and develop a model for predicting the effects of education and training on the security awareness and the security culture for improving the security effectiveness in the healthcare domain. An exploration through on-line search has been carried out among the various search databases such as ACM Digital Library, AISeL, EBSCO, ELSEVIER, IEEE Xplore, PUBMED, SCOPUS, and SPRINGER. Keywords such as 'Security Awareness', 'Security Culture', and 'Education and Training' are inputs for the search. In the following, there is the discussion of the role of human factors as the threats to HIS.

2 An Overview of Literature to Sources of Threats to HIS:

In spite of many attempts in providing security in HIS, data security breaches in health care organizations have continued to increase and number of threats in HIS area has increased dramatically in recent years (Brady, 2011).

Studies show that between 2006 and 2007 in hospitals alone, more than 1.5 million names were exposed to data breaches (HIMSS Analytics, 2008). In addition, the results of 2010 Healthcare Information and Management Systems Society Security Survey suggests that the reports of more than 110 healthcare organizations have shown the loss of sensitive Protected Health Information or Personal Identifying Information affected over 5,306,000 individuals since January 2008and damages from patient information lost top $6 billion per year in 2010 (Sedlack and Tejay, 2011). They were received as theft (stolen laptops, computers, or media), loss or negligence by employees or third parties, malicious insiders, system hacks, web exposure, and virus attacks (HIMSS Analytics, 2010). Moreover, health care organizations have sustained losses not because of inadequate or faulty technology, but rather by users of technology and faulty behavior in numerous data breaches (Appari and Johnson, 2010).

Moreover, viruses and spyware attacks, hackers and intruders place in external threat to IS (Samy *et al*., 2009). Some researchers categorized risks to hospitals as the internal or external threats and found that employees' ignorance, curiosity, recklessness, inadequate behavior, taking someone else's password and giving the password to other employees are the some of the internal threats to HIS. Moreover, viruses and spyware attacks, hackers and intruders are placed in external threat to IS (Samy *et al*., 2009). However, most organizations tend to focus on the vulnerabilities to external threats and have used technical solutions to improve the security of their information system (Parks *et al*., 2011). Many studies suggest that any security breach or security problem is not only related to technology, but it is actually associated more or less with the human factors (Eminağaoğlu *et al*., 2009). Consequently, since most internal security breaches in HIS continue to occur by legitimate users, and people's behavior is a major source of threats to be various IS so, security cannot be achieved only through technological tools (Herath and Rao, 2009). According to (2008), because information security is more of a human problem than a pure technical problem, so now non-technological aspects of information security such as education and awareness must be considered together with technical aspects.

To support these findings, in the previous study, the authors have identified more than 70 threats to HIS and have proved that threats caused by human in the role of users' technology play a big proportion in many threats to HIS (Bakhtiyari Shahri and Ismail, 2012a). References (Asai and Fernando, 2011) prove that human factors are the cause of 80% of privacy breach incidents, and (2009) also confirm that human errors have a large proportion in privacy breaches in the United States. In addition, Published academic of Global Security Survey by Deloitte (2007), found that 91% of participants are concerned about the employees' security weaknesses, and that human factors known as the main reason of the information security failures by 79% of participants (Padayachee, 2012). Moreover, a most people do not feel hurt while they do not see any threat (Asai and Fernando, 2011), according to Figure 1 which shows a brief model on the role of human in threats to HIS, the human is at the center of different threats to HIS security (Bakhtiyari Shahri and Ismail, 2012a). Therefore, HIS users need to be informed and educated about the risk perception biases and understand the magnitude or implications of potential security breaches.

Education and training started emerging as an important cultural tool because they can provide awareness of potential risks and the organization's practices in HIS security. However, training sessions tend to be informational and not integrated into the users' daily activities, which lead to disciplinary actions (Mohan and Razali Raja Yaacob, 2004). Thus, this gap needs to be bridged for an appropriate and effective training (Parks *et al*., 2011).

The rest of study explains the role of education and training in cultivating of security culture and user's security awareness about the threats to HIS.

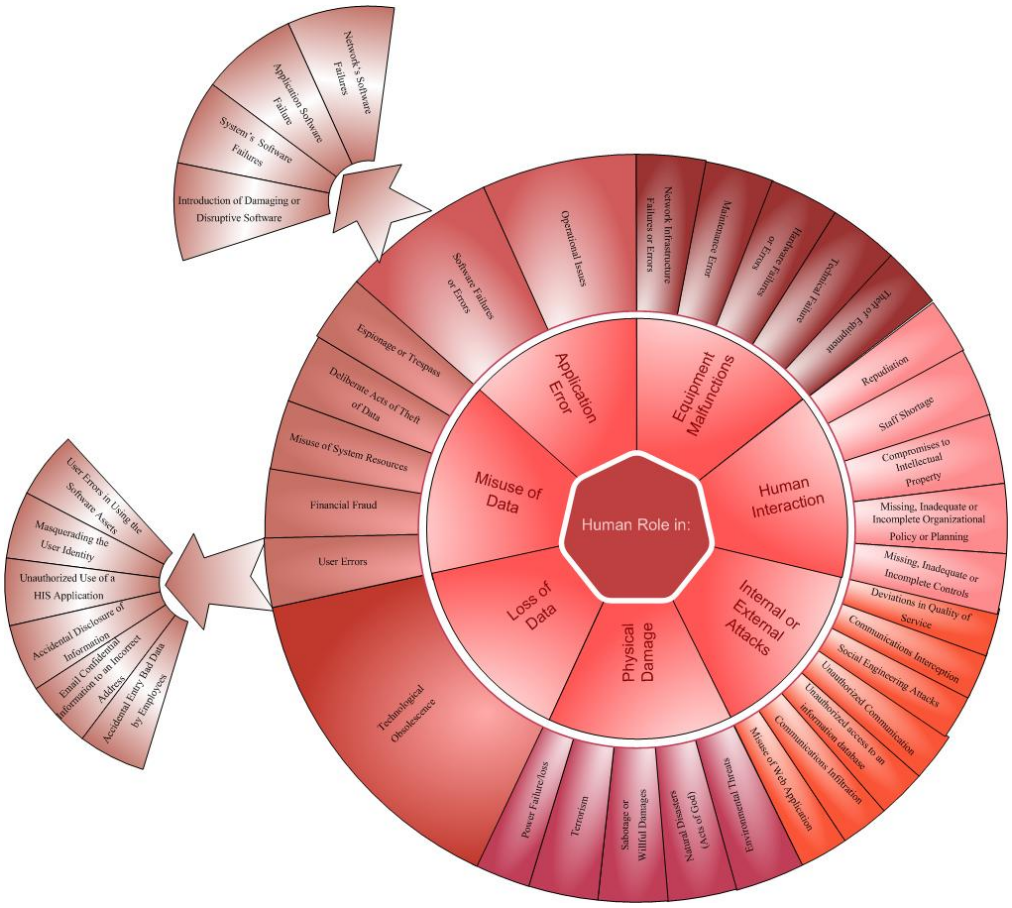

Fig. 1: A brief model for the role of human in threats to HIS

3-Security Effectiveness in 'HIS' Through Education and Training:

The security effectiveness of IS was known by Straub (Straub, 1990) as the ability of systems to provide enough security to protect their assets against different threats such as "the unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against hardware, programs, data, and computer service". In addition, increased risks due to security problems have led to increased security awareness for systems' administrators to provide an effective security for their IS (Dhillon and Backhouse, 2001).

However, more recently researchers have turned to realize that technology tools alone are not able to provide the security of IS, but it depends on technology, processes and people (Herath and Rao, 2009). So, healthcare organizations should implement HIS security effectively by consideration of all the required components of security (Monk *et al*., 2009).

Lacking of security awareness and security culture can be due to the lacking of knowledge about security, as people may not understand the seriousness of the potential threats, and the associated need for security procedures. For example, users may have an inadequate knowledge of what constitutes a secure password, and very few users have understood how passwords could be cracked. Hence, users often have chosen very insecure passwords, without realizing that they were doing so (Parsons *et al*., 2010).

In addition, researchers believe that people remain the weakest link for information security because they are not aware of the risks involved with information technology. Lacking of knowledge about the threats to information security is the main reason for underestimating the level of security awareness in HIS. It would seem that security awareness is an effectiveness parameter to reduce of numerous data breaches by threats. Awareness of the risks and safeguards by education and training is a significant factor in users' beliefs about the security of IS, and it is the first line of defense against different threats to HIS (Goodhue and Straub, 1991).

Besides, the literature on the threats to HIS has identified that culture, and awareness are the two important human factors in HIS security. Therefore, it is necessary to establish an acceptable level of security awareness and security culture among employees as the basic strategy to promote the security of information assets (Eminağaoğlu *et al.*, 2009).

Educating the users about information protection may solve several basic problems associated with information security awareness and culture. It can improve these factors toward security effectiveness in the healthcare domain (Monk *et al*., 2009).

Essentially, employees should be provided with education and training to have the culture and awareness about security from the beginning of employment within an organization, and this training should be improved and assessed regularly.

This study proposes that the education and training is a significant factor which can affect the HIS security effectiveness through improving of security awareness and security culture of HIS users. Therefore, next sections will discuss the place of security awareness and security culture of users in HIS security; it will also investigate the role of education and training to improve these human factors.

3.1 Security Awareness through Education and Training:

Awareness is an effective tool to decrease security incidents; awareness makes users aware of the results of their actions and informs employees about potential threats (Lacey, 2010). It is also used to stimulate, motivate and refresh employees' knowledge to ensure what they are needed to do every day in their work (Peltier, 2005). Awareness includes perhaps the greatest non-technical measures available as the usability features of information security in HIS, which can mitigate information security risks (Yeratziotis *et al*., 2011). With security awareness all employees are informed on the rules, regulations regarding securing, and consequences to their actions within an organization (Yeratziotis *et al*., 2011, Khan *et al*., 2011).

Researchers believe that people remain as the weakest link for information security because they are not aware of the risks involved by information technology. Educating users about information protection may solve several basic problems associated with information security awareness (Monk *et al*., 2009).

Reference (Furnell *et al*., 2006) have highlighted the need for security awareness. In the mentioned study in order to determine the users' correct perception about security features in popular software and applications, the result from a survey of over 340 end-users was investigated. The results showed that over 30% of cases were related to lack of security awareness. Furthermore, an exploratory study at a hospital of Malaysia to categorize threats to HIS showed that awareness and understanding of security threats associated with patient data for HIS's users were needed (2011). In addition, a comparing of EHR information security requirements in Australia, Canada, England and U.S.A to find a new model for the guarantee to the security of EHRs showed that the majority of subject countries emphasized on security awareness of users (2009). This means that, people with the higher security awareness level are more aware of the potential abuse and will feel more certain about the absence of satisfactory in security of HIS (Chen *et al*., 2008). Moreover, since lacking of knowledge about the threats to information security is the main reason for underestimating the level of security awareness in HIS, it is necessary to establish an acceptable level of security awareness among employees as the basic strategy to promote the security of information assets (Eminağaoğlu *et al*., 2009).

Certainly, awareness about the risks and safeguards by education and training is a significant factor in user's beliefs about security of IS, and it is the first line of defense against different threats to IS (Goodhue and Straub, 1991).

It would seem that security awareness is an effective parameter to reduce the numerous data breaches by threats. Therefore, security awareness through education, is also strongly recommended for HIS organizations to educate their users to be aware of security issues (Ng *et al*., 2009). Recently, authors have confirmed that adequate security training is required to improve the information security awareness among all kinds of IS's users such as stakeholders of HIS (Ahlfeldt, 2005, Albrechtsen and Hovden, 2010, Figg and Kam, 2011). Consequently, there is a significant relationship between security awareness and education and training in HIS.

Researchers believe that people remain as the weakest link for information security because they are not aware of the risks involved by information technology. Educating the users about information protection may solve several basic problems associated with information security awareness (Monk *et al*., 2009). Improving of security within the healthcare organization by adequate education and training can increase the basic knowledge and judgment of users about information security; and it can help to prevent of the human errors and carelessness, but little empirical evidence supported these claims (D'Arcy *et al.*, 2009).

Reference (Van Niekerk and Von Solms, 2007) proved that since users are often ignorant of the magnitude of their actions towards information systems, several of risks cannot be prevented if the users of systems are not educated to act securely. They also confirmed that creating a every user's awareness needs training program. In another study (Thomson and Von Solms, 1998) users of IS categorized to End User, IT Personnel, and Top Management; it was emphasized that different users need to be educated in information security awareness in different profiles. Training staff adequately in IT security is an important part of the security awareness and solving the complex information security issues need to awareness, through education (Stander *et al*., 2009).

Most studies in the security awareness discuss about the concept in terms of implementation of a training program to increase the security awareness of end users (Peltier, 2005). Therefore, proper information security

awareness through education is necessary for HIS (Rezgui and Marks, 2008, Monk *et al*., 2009) to ensure that all users are aware of information security threats and it concerns about the course of their normal work (Rezgui and Marks, 2008).

Security Culture through Education and Training:

Providing the security of HIS is not the only technical problem and application of technology alone will not provide the solutions. Therefore, HIS should focus more on the human facet of security. Users' security culture of as the human-social factor is one of the key issues relating to insider threats to information security t is the requirement for HIS security (Colwill, 2009). To supporting this, UK Government reported that 95% of data loss in UK is due to the cultural factors of people (Filho *et al*., 2011, Colwill, 2009).

Since security culture involves all the social and cultural measures that support technical security measures, security of patients' information has become the most noticeable characteristic as the basis of daily activities of employees (Schlienger and Teufel, 2003). Therefore, it is necessary to have a special attention to the information security culture in HISs (Da Veiga and Eloff, 2007, Brady, 2011). To achieve this aim, security managers need to take time to understand the impact of human factor as an element of organizational culture on the information security (Kiely and Benzel, 2006).

Furthermore, Filho, Souza *et al*. (Filho *et al*., 2011) discussed and evolved the impacts of culture in security policy's adherence. They found that understanding human nature and culture is still a key success factor to information. In spite of this fact that information security is an issue of growing importance in HIS (Appari and Johnson, 2010) and that culture of user influences the success of the information security program [21], information security culture is still at the beginning and paves the early steps of development (Alnatheer and Nelson, 2009).

It is important to note that security in IS can be effective if it is regarded by users, training is vital to create a culture of privacy and security at HIS (Ontario, 2008). Shaw, Chen *et al*. (Shaw *et al*., 2009) mentioned the importance of permanently increase of information security culture in organizations. Likewise, Thomson and Solms (Thomson and von Solms, 2005) proved that training needs to be provided by organization to improve a conducive culture to the protection of information assets.

Therefore, changing employees' behavior and attitude positively to information security by promotion awareness of users would increase the organization's security culture and thus improve the effectiveness of the IS security (Dzazali and Zolait, 2012).

In addition, to protect information assets in each organization, insiders must change their behavior by security cultural values. This requires a greater focus on education of employees (Colwill, 2009). Consequently, since security culture actually must be seen in user's behaviors in an effectiveness information security program (Shaw *et al*., 2009), education and training are necessary for creation a culture of security for end-users within the health care organization (Dzazali and Zolait, 2012).

Conceptual Framework Developments:

The conceptual model derived from the findings of this investigation has been used to predict the influence of education and training to improve the users' culture and awareness about HIS security. Figure 2 presents the conceptual model for this research, which has been developed from the literature.

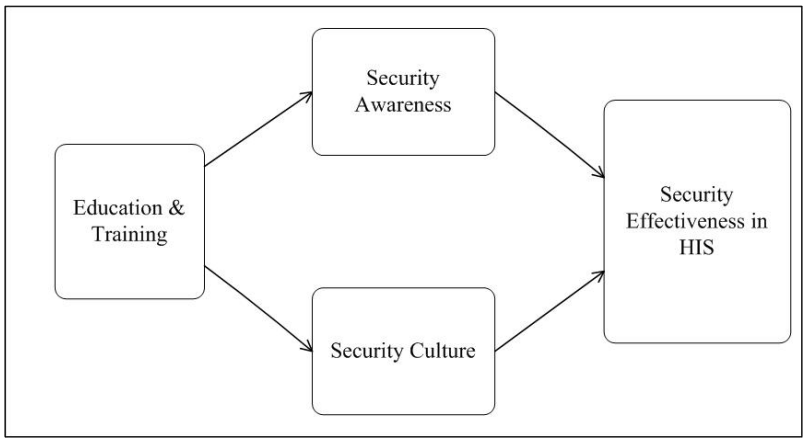

Fig. 2: The proposed model for security effectiveness in HIS through education and training

Conclusion:

The author's goal in conducting this investigation was to identify the issues and important human factors involving information security awareness, information security culture, and education and training that help the implementation and adoption of HIS security effectively. So, by considering the human activity as the core of threats to HIS information security (Bakhtiyari Shahri and Ismail, 2012b), users need education and training to improve of their awareness and culture about security issues in the healthcare domain.

This work-in-progress study will investigate HIS health care domain. The result of this study may provide some insights to both researchers and professionals, who are interested in conducting research in security of HIS.

ACKNOWLEDMENT

This study was funded by the Research University Grant from Universiti Teknologi Malaysia (UTM) and Ministry of Higher Education (MOHE) Malaysia with the project number Q.K 130000.2138.01H98.

REFERENCES

Ahlfeldt, R.M., 2005. Information Security in a Heterogeneous Healthcare Domain. 4th Security Conference. Las Vegas, USA.

Albrechtsen, E. & J. Hovden, 2010. Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. An Intervention Study. Computers & Security, 29: 432-445.

Alnatheer, M. & K. Nelson, 2009. Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. 7th Australian Information Security Management Conference. Perth, Western Australia.

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

Asai, T. & S. Fernando, 2011. Human-Related Problems in Information Security in Thai Cross-Cultural Environments. Contemporary Management Research, 7: 117-142.

Bakhtiyari Shahri, A. & Z. Ismail, 2012a. Human Factors as the Biggest Threats to Security of Health Information Systems. International Journal of Communications and Information Technology (IJCIT), 2.

Bakhtiyari Shahri, A. & Z. Ismail, 2012b. A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS. Journal of Information Security, 3: 169-176.

Brady, J.W. Year, 2011. Securing Health Care: Assessing Factors That Affect HIPAA Security Compliance in Academic Medical Centers. In: 44th Hawaii International Conference on System Sciences, 4-7 Jan. 2011 2011 Kauai, HI. IEEE, 1-10.

Chen, C.C., R.S. Shaw, & S.C. Yang, 2008. Year. The Efficacy of a Situational Approach on Increasing Security Awareness of General Users in Different Culture. In: 39th Annual Meeting of the Decision Sciences Institute, USA. pp: 2411-2416.

Colwill, C., 2009. Human Factors in Information Security: The Insider Threat–Who Can You Trust These Days? Information Security Technical Report, 14: 186-196.

D'arcy, J., A. Hovav, & D. Galletta, 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, 20: 79-98.

Daveiga, A. & J.H.P. Eloff, 2007. An Information Security Governance Framework. Information Systems Management, 24: 361-372.

Dhillon, G. & J. Backhouse, 2001. Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. Information Systems Journal, 11: 127-153.

Dzazali, S. & A.H. Zolait, 2012. Assessment of Information Security Maturity: An Exploration Study of Malaysian Public Service Organizations. Journal of Systems and Information Technology, 14: 2-2.

Eminağaoğlu, M., E. Ucar, & Ş. Eren, 2009. The Positive Outcomes of Information Security Awareness Training in Companies – A Case Study. Information Security Technical Report, 14: 223-229.

Farzandipour, M., M. Ahmady, F. Sadoughi, & I. Karimi, 2009. Designing a Model for Security Requirements of Electronic Health Records in Iran. JQUMS, 13: 79-86.

Farzandipour, M., F. Sadoughi, M. Ahmadi, & I. Karimi, 2010. Security Requirements and Solutions in Electronic Health Records: Lessons Learned from a Comparative Study. Journal of Medical Systems, 34: 629-642.

Figg, W.C. & H.J. Kam, 2011. Medical Information Security. International Journal of Security (IJS), 5: 22.

Filho, E.L., J.H.P. Souza, A.T. Chaves, G.T. Hashimoto, & P.F. Rosa, 2011. Year. The Impact of Corporate Culture in Security Policies – A Methodology. In: The Seventh International Conference on Networking and Services (ICNS 2011), May 22-27, 2011 2011 Venice/Mestre, Italy. 98-103.

Furnell, S.M., A. Jusoh, & D. Katsabas, 2006. The Challenges of Understanding and Using Security: A Survey of End-Users. Computers & Security, 25: 27-35.

Goodhue, D.L. & D.W. Straub, 1991. Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security. Information & Management, 20: 13-27.

Herath, T. & H. Rao, 2009. Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. Decision Support Systems, 47: 154-165.

Himss Analytics, 2008. The 2008 HIMSS Analytics Report: Security of Patient Data. Technical Report.

Himss Analytics, 2010. The 2010 HIMSS Analytics Report: Security of Patient Data. Technical Report.

Huang, D.L., P.L. Patrick Rau, & G. Salvendy, 2010. Perception of Information Security. Behaviour & Information Technology, 29: 221-232.

Khan, B., K.S. Alghathbar, S.I. Nabi, & M.K. Khan, 2011. Effectiveness of Information Security Awareness Methods Based on Psychological Theories. African Journal of Business Management, 5: 10862-10868.

Kiely, L. & T.V. Benzel, 2006. Systemic Security Management. Journal of Security & Privacy, IEEE, 4: 74-77.

Kraemer, S., P. Carayon, & J. Clem, 2009. Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities. Computers & Security, 28: 509-520.

Lacey, D., 2010. Understanding and Transforming Organizational Security Culture. Information Management & Computer Security, 18: 4-13.

Liginlal, D., I. Sim, L. Khansa, & P. Fearn, 2009. Year. Human Error and Privacy Breaches in Healthcare Organizations: Causes and Management Strategies. In: 15th Americas Conference on Information Systems (AMCIS 2009), 2009 San Francisco, California.

MA, Q., A.C. Johnston, & J.M. Pearson, 2008. Information Security Management Objectives and Practices: A Parsimonious Framework. Information Management & Computer Security, 16: 251-270.

Mohan, J. & R. Razali Raja Yaacob, 2004. The Malaysian Telehealth Flagship Application: a national approach to health data protection and utilisation and consumer rights. International Journal of Medical Informatics, 73: 217-227.

Monk, T., J. Van Niekerk, & R. Von Solms, 2009. Year. Concealing the Medicine: Information Security Education through Game Play. In: Information Security South Africa (ISSA), 2009 Johannesburg. ISSA, 467-477.

Narayana Samy, G., R. Ahmad, & Z. Ismail, 2010. Security Threats Categories in Healthcare Information Systems. Health Informatics Journal, 16: 201-209.

NG, B.Y., A. Kankanhalli, & Y.C. Xu, 2009. Studying Users' Computer Security Behavior: A Health Belief Perspective. Decision Support Systems, 46: 815-825.

Ontario, 2008. The eHealth Ontario Privacy and Security Employee Standard of Conduct. Privacy and Security Standard of Conduct, Document Identifier: 00990.

Padayachee, K., 2012. Taxonomy of Compliant Information Security Behavior. Computers & Security, 31.

Parks, R., C.H. Chu, & H. XU, 2011. Year. Healthcare Information Privacy Research: Iusses, Gaps and What Next? In: 17th American Conference on Information Systems (AMCIS 2011), 4-8 August 2011 Detroit.

Parsons, K., A. Mccormac, M. Butavicius, & L. Ferguson, 2010. Human Factors and Information Security: Individual, Culture and Security Environment. Defence Science and Technology Organisation (DSTO), 2010**,** 1-45.

Peltier, T.R., 2005. Implementing an Information Security Awareness Program. Information Systems Security, 14: 37-49.

Rezgui, Y. & A. Marks, 2008. Information Security Awareness in Higher Education: An Exploratory Study. Computers & Security, 27: 241-253.

Samy, G.N., R. Ahmad, & Z. Ismail, 2009. Year. Threats to Health Information Security. In: 5th International Conference on Information Assurance and Security of the IEEE IAS, 8-20 August 2009 2009 Xi'an. IEEE, 540-543.

Samy, G.N., R. Ahmad, & Z. Ismail, 2011. Year. Health Information Security Guidelines for Healthcare Information Systems. In: ISHIMR 2011, 8-9 September 2011 2011 Zurich, Switzerland. 10.

Schlienger, T. & S. Teufel, 2003. Year. Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. In: 14th International Workshop on Database and Expert Systems Applications, pp: 405-409.

Sedlack, D.J. & G.P.S. Tejay, 2011. Year. Improving Information Security Through Technological Frames of Reference. In: Southern Association for Information Systems Conference, Atlanta, GA, USA. 153-157.

Shaw, R.S., C.C. Chen, A.L. Harris, & H.-J. Huang, 2009. The Impact of Information Richness on Information Security Awareness Training Effectiveness. Computers & Education, 52: 92-100.

Stander, A., A. Dunnet, & J. Rizzo, 2009. Year. A Survey of Computer Crime and Security in South Africa. In: Information Security South Africa (ISSA), Johannesburg. ISSA, pp: 217-226.

Straub, D.W., 1990. Effective IS Security. Information Systems Research, 1: 255-276.

Thomson, K.L. & R. Von Solms, 2005. Information Security Abedience: A Definition. Computers & Security, 24: 69-75.

Thomson, M. & R. Von Solms, 1998. Information Security Awareness: Educating Your Users Effectively. Information Management & Computer Security, 6: 167-173.

Van Niekerk, J. & R. Von Solms, 2002. Year. A Web-Based Portal for Information Security Education. In: Information Security South Africa (ISSA), 10-12 July 2002 2007 Johannesburg, South Africa. ISSA, 1-10.

Williams, P., 2009. Capturing Culture in Medical Information Security Research. Methodological Innovations Online, 4: 15-26.

Yeratziotis, A., D. Van Greunen, & D. Pottas, 2011. Year. Recommendations for Usable Security in Online Health Social Networks. In: 6th International Conference on Pervasive Computing and Applications (ICPCA), 26-28 Oct. 2011 2011 Port Elizabeth. IEEE, pp: 220-226.