Jurnal Teknologi

Full paper

Security Culture and Security Awareness as the Basic Factors for Security Effectiveness in Health Information Systems

Ahmad Bakhtiyari Shahri[a*], Zuraini Ismail[b], Nor Zairah Ab. Rahim[b]

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

*Corresponding author: bsahmad2@live.utm.my

Article history

Received :4 April 2013
Received in revised form :
25 July 2013
Accepted :15 October 2013

Abstract

The use of Information and Communications Technology (ICT) in healthcare domains contributes to an increased complexity of the problems related to the security of Health Information Systems (HIS). This is primarily may be due to the introduction of human behaviors. In spite of many attempts in providing security for HIS, security incidents remain to continue due to human factors. The key to achieve security effectiveness of information systems is through the nurturing of HIS users security awareness and culture towards patients' data. Hence, addressing the role of human behavior is the main focus for this study. Based on the secondary data resources, a theoretical model is proposed according to users' awareness and users' culture for HIS security. This work-in-progress study attempts to highlight the HIS users' behaviors in enhancing the security effectiveness for HIS.

Keywords: Health information system; security culture; security awareness; security effectiveness

1.0 INTRODUCTION

The healthcare industry has expanded the use of Information and Communications Technology (ICT) to provide better care and help for cost reduction. Definitely, use of ICT in healthcare domains contributes to an increased complexity of the problems related to Health Information System (HIS), in particular, by introducing concepts such as human errors. Since the start of the information age, the sentence that ''Computers do not commit crimes, people do.'' has been quoted in numerous security presentations [1].

In addition, due to increased data security breaches in health care organizations in recent years, security effectiveness of health information systems has always been one of the hottest topics for researchers [2]. A large number of healthcare organizations reported data security breaches in 2009 and 2010 through the employees' failure to comply with organizational information security guidelines [3].

National surveys confirmed the high number of data security breaches against health information resources that were received by human factors [4, 5]. Therefore, to guarantee security and privacy of patients' data, healthcare organizations should pay more attention to the HIS security effectiveness based on human behavior [6, 7].

In spite of the fact that the key to achieving HIS security effectiveness is through human behaviors, the revising of literatures identifies that addressing the role of users' behaviors such as security culture and security awareness are the main problems for the security effectiveness of IS in healthcare organizations [2, 8, 9].

However, healthcare organizations have sustained losses not because of insufficient or faulty technology, but rather by users of technology and also faulty behaviors of users [10]. Most existing methods for security effectiveness for information systems in health care organizations were based on technical viewpoint [11, 12]. According to UK Government report, only 5% of all data loss in UK are due to technology issues and 95% is related to security culture of people [13].

Moreover, researchers have concluded that the largest security threat facing health organization is the insecure behavior of its own IS users[14-16]. Information about the causes of these behaviors is lacking, and according to Teer *et al.* [17], research is required to identify the security culture and security awareness that relate to the security behavior's users. In addition, prior researches that examined the security behavior of IS users have mainly been focused on the analysis of inappropriate security behaviors [18, 19]. Additional researchers also examined the influence of organizational factors such as organizational size, top management support, security policy, and industry type on the security effectiveness for IS [2, 20]. Some studies have also focused on information security risk analysis method to identify a vulnerability of the security breach in HIS [21-23]. These studies, however, have been considered limited in addressing human factor relating to IS security behaviors [24]. Other existing methods depend largely on IT professionals to conduct the framework for security of IS [20, 25, 26].

As a result, users without the security culture and the security awareness seem to be the greatest threats to security of health information systems and current approaches towards users' behaviors in information security have not provided effective security for health information systems. Hence, there is a lack of framework for security of health information systems based on the security culture and the security awareness of users. This study tries to introduce the comprehensive framework for security effectiveness of health information systems based on security culture and the security awareness.

2.0 RESEARCH METHODOLOGY

By use of secondary data resources it has been found that security effectiveness of HIS is associated more with the culture and awareness of users about information security. An exploration through on-line search has been carried out among the various search databases. Therefore, the first findings of this study are identifying the security culture and the security awareness as the important factors for security effectiveness in health information systems. Then, analysis and revision of literature show a clear need for a framework that includes security awareness and security culture. The study proposes a framework based on mentioned factors to implement the security effectiveness in HIS.

3.0 SECURITY EFFECTIVENESS FOR INFORMATION SYSTEM

Measuring the effectiveness of security in information systems (IS) is an issue that has seriously been questioned among academics and practitioners. The effectiveness of security measures in reducing the overall risk to information in organizations had been studied extensively over the years. According to Straub [27], IS security effectiveness is the ability of IS security measure to protect against unauthorized or deliberate misuse of IS assets of people.

One of the first models on IS security effectiveness has been provided by Straub [27]. The model was based on the criminological theory of General Deterrence (GDT), that investigated on whether a management decision in IS security result is more effective control of computer abuse. Data gathered through a survey of 1211 randomly-selected organizations indicates that security countermeasures that include deterrent administrative procedures and preventive security software will result in lower computer abuse.

Other researchers developed the Straub' model and have used GDT as a theoretical perspective in examining the effectiveness of various security countermeasures in different environments [20, 25, 26, 28].

In a-depth study Kankanhalli *et al.* [20] proposed a conceptual model of IS security effectiveness. Their theoretical model includes organizational factors such as Organizational size, Top management support, and Industry type. Based on 63 IS managers' responses from multiple professional organizations, they also found that greater deterrent efforts and preventive measures can increase IS security effectiveness.

Following Straub (1990), D'Arcy and Hovav [25] used the term ''security countermeasures'' to collectively describe procedural and technical controls. By use of an extended deterrence theory model, certain controls for IS misuse were identified. Their model was tested by an online survey instrument for data collection from 269 users in eight companies. They suggested that three practices deter IS misuse: user awareness of security policies; security education, training, and awareness (SETA) programs; and computer monitoring. The result showed that security awareness is the most countermeasures against human factor in threats to IS. Although the model investigated the role of individual factors on information security, the results were not consistent misuse behaviors examined, and there is a need for different groups of computer' users, different security approaches are considered.
The majority of the mentioned studies has suggested the model extension by organizational factors incorporation like an organizational culture for future work. Review of literature, however, identifies a number of security frameworks according to organizational factors.

In a new way, some researchers emphasize that through implementing all the required information security components, organizations must govern information security effectively [2, 29-31]. Different information security components such as human factors, organizational factors, and technical factors can be used to compile a new comprehensive information security framework.

Besides that, Da Veiga and Eloff [30] focused on employee behavior and have investigated security effectiveness in terms of security culture by presenting a framework to develop an information security culture in an organization. Similarly, Hearth and Rao (2009) showed that end-user security behaviors that cannot be achieved through just technological tools are an important part of enterprise-wide information security. Both intrinsic and extrinsic motivators can influence security behaviors of users. Based on 312 employee responses from 77 organizations, they assessed the effectiveness of the security model consist of various motivating factors such as penalties, pressures and perceived contribution that encourages information security behaviors in organizations. The study mentioned that creating a general culture that fosters security is a better strategy in information security [31].

A security effectiveness framework for information system for higher-education institutions proposed by Ismail *et al.* [32]. The framework was adapted from ISO 27001, MyMIS and COBIT standards. Security policy, risk management, access control, awareness program and training, and compliance were identified in their framework as the important constructs . Moreover, by the use of mix method, they identified security awareness as an important factor in the information security framework for Higher Education Institutions (HEI). Interviews have been done with IT-expert staff and personnel in-charge of developing the Information Security framework in four HEIs selected located in the Klang Valley of Malaysia. Moreover, they used a survey to examine the IT personnel perceptions on the existing proposed framework.

Brady (2011) suggested a theoretical model for HIPAA security compliance in U.S.A academic medical centers. The model is based on management support, security awareness, security culture, and computer self-efficacy. The results showed that security awareness, management support, and security culture were important predictors of security effectiveness and security behavior, with security awareness as the most important predictor.

In a case study at a university, Ayyagari and Tyks 33 addressed the data breaches that are caused by lax security policies and includes an element of social engineering. The results showed that Top Management Support, Policies, and Awareness at the university improve security effectiveness. Table 1 is the summary of related work in IS security effectiveness.

Literature review of different frameworks on IS security-related works have identified security culture and security

awareness as the significant factors that contribute to security effectiveness.

Table 1 Information systems security related works

Author(s) / Year	Instrument	Important Factors	
		Security Culture	Security Awareness
Ayyagari and Tyks (2012)	Case studies at university		√
Benhocine (2012)	A technical solution to provide a theoretical model.		√
Brady (2011)	Web based Survey	√	√
Huang *et al*. (2011)	Survey of 64 IT users		√
Sushma *et al*.(2011)	A survey of 54 students enrolled in master's degree programs		
Ismail *et al*. (2010)	Interview and survey of four Malaysian Higher Education Institutions (HEI)		√
Niekerk and Solms	Theoretical	√	√
D'Arcy and Hovav (2009)	Survey of 238 participants in two groups of professionals in eight organizations across the U.S.		√
Da Veiga and Eloff (2009)	Survey of 3000 employees in South Africa	√	
Knapp *et al*. (2007)	Survey of 220 information security practitioners	√	√
Chang and Ho (2006)	Survey of 59 organizations in Taiwan		
Kankanhalli *et al*. (2003)	Survey of IS managers from various sectors of the economy		√

3.1 Information Security Culture

Culture may be described as a set of ideas, values, understandings, and norms shared by an organization members [34]. Moreover, culture offers a common language to promote the understanding of policy and procedure and helps to implement the security practice [35]. Hence, security culture is defined as "A focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks" [36]. Without a security culture, it is likely that employees may be aware of existing and potential risks, but still behave in an insecure manner [37].

According to UK Government Report, only 5% all the data loss in the UK is because of technology issues even as 95% is by reason of cultural factors of people [13]. Therefore, researchers have pointed out that security culture is an important factor in maintaining an adequate level of information security in organizations [38]. It has even asserted that only a significant change in security culture can reduce the number of security breaches experienced [39].

However, it is necessary to establish a security culture as the key to manage human factors in all organizations [40]. Therefore, to achieve this aim, security managers need to take time to understand the cultural construct on regarding the implementation of security effectiveness of information systems in organizations [41].

In-depth study by Da Veiga and Eloff [30] showed that information security culture can diminish the risks to information assets and decrease the risk of employee misbehavior and harmful interaction with information assets. They suggested a framework for promoting information security culture in organization in three levels. To design an instrument for assessment of information security culture a formal survey methodology was used. The proposed model was tested in a South African firm with approximately 3000 employees.

The most important thing in result of the literature review in this study is that although security culture is a multidimensional concept, it has often been investigated in a simplistic manner and only a few studies have identified its dimensions [38]. Moreover, it is clear that the security culture is one of the necessary factors that may be considered in the implementation of an effective information security program in each IS [30, 40, 42].

Table 2 Security culture in information systems

Author(s) / Year	Instrument/ Sample	Findings
Coen (2012)	Survey of 300 respondents	The culture encourages user's awareness and reduces information security risks.
Brady (2011)	Online survey of 76 health care professionals	Security culture is a significant predictor of security effectiveness and security behavior.
Figg and Kam (2011)	Qualitative positivist approach for the exploration, classification, and hypothesis development	Attitude and Awareness, Power Relation between Users, Collective Norms, Values, and Knowledge, and Assumptions and Beliefs are the components of security culture.
Filho *et al*. (2011)	Theoretical	The article discusses the impacts of culture in security policy adherence.
Appari and Johnson (2010)	Critical survey on information security in healthcare	Security culture plays a significant role in health information security.
Da Veiga and Eloff (2010)	Survey methodology to assess the information security culture in a South African firm with approximately 3000 employees	The study presented a framework for cultivating of information security culture in organization in three levels.
Gwen Greene and D'Arcy (2010)	Data collection had been done by two online surveys. The sample consisted of 127 employed working professionals taking MBA classes at two mid-Atlantic U.S. universities.	Security culture is a multidimensional construct consisting of top management commitment to security, security communication, and computer monitoring that has a positive effect on users' IS security.
Van Niekerk and Von Solms (2010)	Theoretical Model	Establish a security culture is the key to managing the human factors of the organization.
Alnatheer and Nelson (2009)	In a theoretical method, it suggested a framework for information security culture in Saudi Arabia.	Security Awareness, Training Programs, Information Security Policy, Top Management Support, Compliance, Information Security Risk Analysis, and Organizational Culture influence on security culture.
D'Arcy and Greene (2009)	Survey of computer-using professionals in organizations in mid-Atlantic U.S. region.	There is a strong relationship between security culture and compliant user's behavior.
Chang and Lin (2007)	Survey of 108 senior IT managers and professionals in various industries.	Organizational culture has a positive influence on security management effectiveness.
Da Veiga and Eloff (2007)	Theoretical	Management support and security awareness need for an acceptable level of information security culture.
Von Solms and von Solms (2004)	Theoretical	Education and communication efforts are important for cultivating of information security culture.

3.2 Information Security Awareness

Information security awareness can be defined as the amount of perceptions of the users about the importance of information security, security level required for the organization, personal and individual responsibility in security, and acts accordingly [43]. Awareness informs employees about the consequences of their actions and also makes users conscious of possible threats and urgent security risks, making it an efficient device to decrease incidents [37]. It is also applied to motivate, inspire and revive the knowledge of the staff to make sure what they are needed to carry out in their everyday routines of work [44].

In the IS literature, security awareness has been examined as an effecting successful in perception of information security [45, 46], impacting users' behaviors [43], influencing on security culture [30, 39, 42], impact on computer self-efficacy [2], and impacting managerial [47], and influencing on threats to IS [21, 25].

Some of the recent studies examined the key issues relating to insider threats to information security [13, 21] and found that security awareness is perhaps the greatest non-technical measures available as the usability features of IS security. However, Chang *et al*. (2006)the noted that effective information security could consider both technical and non-technical security threats. To address information threats, security awareness and security regulations ought to be monitored to guarantee a secure and proper setting for the information assets of a firm. Based on specific IS circumstances, alertness of the required security principles is basic to the security [48] .

The results of some studies have shown that security awareness is an important determinant in achieving security effectiveness.

Table 3 Security Awareness in information systems

Author(s) / Year	Instrument/ Sample	Findings
Brady (2011)	Online survey of 76 health care professionals	Security awareness is a significant predictor of security effectiveness and security behavior.
Huang *et al*. (2011)	Survey questionnaire of 64 customers of e-banking.	Perception of information security can be enhanced by changing users' awareness.
Samy *et al*. (2011)	Exploratory study in a hospital in Malaysia.	Awareness of the security threats associated with patients' data for HIS's users were needed.
Yeratziotis (2011)	A formative usability evaluation of security and privacy features of Google Health and MedHelp websites.	Security awareness is the critical feature in the evaluation of security and privacy of online Health Social Networks.
Appari and Johnson (2010)	Critical survey on information security in healthcare.	Security awareness is a effectiveness parameter to cause of numerous data breaches by threats.
Farzandipour *et al*.(2010)	Comparative study about EHR information security requirements of Australia, Canada, England and U.S.A	The majority of subjects countries emphasized on security awareness of users in their framework.
Ismail *et al*. (2010)	Interview with IT-expert staff in 4 HEI and survey of 72 IT personnel.	Security awareness is an important factor in information security of Higher Education Institutions.
Colwill (2009)	Theoretical	Security awareness is the greatest non-technical measures as the usability features of IS security.
D'Arcy *et al*. (2009)	Online survey of 269 users in eight companies.	Security awareness is the most countermeasures against the threats to IS.
Ng *et al*. (2009)	Survey of 134 employees in multiple organizations.	Users need training and awareness programs to be aware of security issues.
Da Veiga and Eloff (2007)	Theoretical	Security awareness is needed for an information security culture.
Knapp *et al*. (2007)	Interview with 220 and surveys of 740 information security professionals in the International Information Systems Security Certification Consortium.	Security awareness influences IS security effectiveness.
Chang and Yeh (2006)	Survey of 109 managers of large Taiwan firms	Security awareness is necessary to achieve the effective security in IS.

3.3 Conceptual Fremework Development

The objective of this study is to identify security culture and security awareness as the basic non-technical factors for IS security effectiveness models in the healthcare domain. According to previous sections, by a review of current approaches towards HIS security and by putting together the literature on security effectiveness, a conceptual framework for the security effectiveness for health information systems was constructed. Figure 1 describes that a relationship may be between security culture and security awareness with security effectiveness in health information systems.

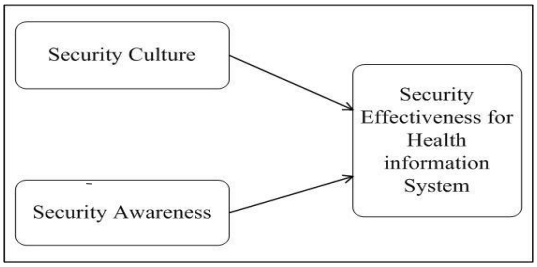

Figure 1 The proposed research framework

4.0 CONCLUSION

Health Information Systems in some countries are still at the beginning; and growing capacity of information technologies in different aspects of health care will produce a need for additional security measures about the guarantee of the security of HIS. In addition, users are the important factor in the chain of health information security. Therefore, it is necessary to notify the HIS managers about the influence of non-technical issues on security of HIS. By using the secondary data resources, a conceptual framework was constructed in addressing the research objective. The extensive search has resulted in two independent variables, namely security culture and security awareness. The results of this study may explain the reasons of importance of security culture and security awareness in establishing the security effectiveness for HIS. Therefore, this work-in-progress will proceed with instrument design and data collection to validate the proposed framework. It may be able to correct the HIS users' behaviors in order to enhance the security of patients' data and also provide some insights to both researchers and professionals, who are interested in conducting research in security of HIS.

Acknowledgement

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

[1] Lacey, D. 2009. *Managing the Human Factor in Information Security: How to Win over Staff and Influence Business Managers*: John Wiley & Sons Ltd.

[2] Brady, J. W. 2011. *Securing Health Care: Assessing Factors That Affect HIPAA Security Compliance in Academic Medical Centers*. in 44th Hawaii International Conference on System Sciences. Kauai, HI: IEEE.

[3] Clearinghouse, P. R. 2010. *Privacy Rights Cearinghouse*: Center for Public Interest Law, University of San Diego.

[4] HIMSS Analytics. 2008. *The 2008 HIMSS Analytics Report: Security of Patient Data*. Technical Report.

[5] HIMSS Analytics. 2010. *The 2010 HIMSS Analytics Report: Security of Patient Data*. Technical Report.

[6] Ma, Q., A. C. Johnston, and J. M. Pearson. 2008. Information Security Management Objectives and Practices: A Parsimonious Framework. *Information Management & Computer Security*. 16(3): 251–270.

[7] Winter, A., R. Haux, E. Ammenwerth, B. Brigl, N. Hellrung, and F. Jahn, *Health Information Systems*, in *Health Information Systems*. 2011, Springer: London. 33–42.

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

[9] Williams, P. 2009. Capturing Culture in Medical Information Security Research. *Methodological Innovations Online*. 4(3): 15–26.

[10] Rotvold, G. 2008. How to Create a Security Culture in Your Organization. *Information Management Journal*. 42(6).

[11] Dimitropoulos, L. and S. Rizk. 2009. A State-Based Approach to Privacy and Security for Interoperable Health Information Exchange. *Health Affairs*. 28(2): 428–434.

[12] Benhocine, A., L. Laouamer, and H. Hadji. 2011. Toward an Efficient Security: A New Methodology for Information Security. *Journal of Economics and Administration*. 1(1).

[13] Colwill, C. 2009. *Human Factors in Information Security: The Insider Threat–Who Can You Trust These Days?* Information Security Technical Report. 14(4): 186–196.

[14] Keller, S., A. Powell, B. Horstmann, C. Predmore, and M. Crawford. 2005. Information Security Threats and Practices in Small Businesses. *Information Systems Management*. 22(2): 7–19.

[15] Whitman, M. E. 2003. Enemy at the Gate: Threats to Information Security. *Communications of the ACM*. 46(8): 91–95.

[16] Ramim, M. and Y. Levy. 2006. Securing E-Learning Systems: A Case of Insider Cyber Attacks and Novice IT Management in a Small University. *Journal of Cases on Information Technology (JCIT)*. 8(4): 24–34.

[17] Teer, F. P., S. Kruck, and G. P. Kruck. 2007. Empirical Study of Students' Computer Security Practices/Perception. *The Journal of Computer Information Systems*. 47(3): 105–110.

[18] Leach, J. 2003. Improving User Security Behaviour. *Computers & Security*. 22(8): 685–692.

[19] Stanton, J. M., K. R. Stam, P. Mastrangelo, and J. Jolton. 2005. Analysis of End User Security Behaviors. *Computers & Security*. 24(2): 124–133.

[20] Kankanhalli, A., H. H. Teo, B. C. Y. Tan, and K. K. Wei. 2003. *An* Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management*. 23(2): 139–154.

[21] Samy, G. N., R. Ahmad, and Z. Ismail. 2011. *Health Information Security Guidelines for Healthcare Information Systems*. In ISHIMR 2011. Zurich, Switzerland.

[22] Maglogiannis, I., E. Zafiropoulos, A. Platis, and C. Lambrinoudakis. 2006. Risk Analysis of a Patient Monitoring System Using Bayesian Network Modeling. *Journal of Biomedical Informatics*. 39(6): 637–647.

[23] Tupa, J. and F. Steiner. 2006. Implementation of Information Security Management System in the Small Healthcare Organization. *Journal of Telecommunications and Information Technology*. (2): 52–58.

[24] Aytes, K. and T. Connolly. 2004. Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organizational and End User Computing (JOEUC)*. 16(3): 22–40.

[25] D'Arcy, J. and A. Hovav. 2009. Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. *Journal of Business Ethics*. 89: 59–71.

[26] Sushma, M., M. Robert, and L. Chasalow. 2011. Information Security Effectiveness: A Research Framework. *Issues in Information Systems*. 7(1): 246–255.

[27] Straub, D. W. 1990. Effective IS Security. *Information Systems Research*. 1(3): 255–276.

[28] Wiant, T. L. 2005. Information Security Policy's Impact on Reporting Security Incidents. *Computers & Security*. 24(6): 448–459.

[29] Da Veiga, A. and J. H. P. Eloff. 2007. An Information Security Governance Framework. *Information Systems Management*. 24(4): 361–372.

[30] Da Veiga, A. and J. Eloff. 2010. A Framework and Assessment Instrument for Information Security Culture. *Computers & Security*. 29(2): 196–207.

[31] Herath, T. and H. Rao. 2009. Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems*. 47(2): 154–165.

[32] Ismail, Z., M. Masrom, Z. Sidek, and D. Hamzah. 2010. Framework to Manage Information Security for Malaysian Academic Environment. *Information Assurance & Cybersecurity*. 2010: 1–16.

[33] Ayyagari, R. and J. Tyks. 2012. Disaster at a University: A Case Study in Information Security. *Journal of Information Technology Education*. 11.

[34] Knapp, K. J., T. E. Marshall, R. K. Rainer, and F. N. Ford. 2006. Information Security: Management's Effect on Culture and Policy. *Information Management & Computer Security*. 14(1): 24–36.

[35] Figg, W. C. and H. J. Kam. 2011. Medical Information Security. *International Journal of Security (IJS)*. 5(1): 22.

[36] OECD. 2002. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*: Organisation for Economic Co-operation Development.

[37] Lacey, D. 2010. Understanding and Transforming Organizational Security Culture. *Information Management & Computer Security*. 18(1): 4–13.

[38] Ruighaver, A. B., S. Maynard, and S. Chang. 2007. Organisational Security Culture: Extending The End-User Perspective. *Computers & Security*. 26(1): 56–62.

[39] D'Arcy, J. and G. Greene. 2009. *The Multifaceted Nature of Security Culture and Its Influence on End User Behavior*. In International Workshop on Information Systems Security Research.

[40] Van Niekerk, J. and R. Von Solms. 2010. Information Security Culture: A Management Perspective. *Computers & Security*. 29(4): 476–486.

[41] Kiely, L. and T. V. Benzel. 2006. Systemic Security Management. *Journal of Security & Privacy, IEEE*. 4(6): 74–77.

[42] Gebrasilase, T. and L. F. Lessa. 2011. Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. *The African Journal of Information Systems*. 3(3): 72–86.

[43] Khan, B., K. S. Alghathbar, S. I. Nabi, and M. K. Khan. 2011. Effectiveness of Information Security Awareness Methods Based on Psychological Theories. *African Journal of Business Management*. 5(26): 10862–10868.

[44] Peltier, T. R. 2005. Implementing an Information Security Awareness Program. *Information Systems Security*. 14(2): 37–49.

[45] Furnell, S. M., A. Jusoh, and D. Katsabas. 2006. The Challenges of Understanding and Using Security: A Survey of End-Users. *Computers & Security*. 25(1): 27–35.

[46] Huang, D. L., P. L. Patrick Rau, G. Salvendy, F. Gao, and J. Zhou. 2011. Factors Affecting Perception of Information Security and Their Impacts on IT Adoption and Security Practices. I*nternational Journal of Human-Computer Studies*. 69(12): 870–883.

[47] Greene, G. and J. D'Arcy. 2010. *Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance*. In Fifth Annual Symposium on Information Assurance. Albany.

[48] Chang, A. J. T., J. Arthur, Q. J. Yeh, and J. Quey. 2006. On Security Preparations Against Possible IS Threats Across Industries. *Information Management & Computer Security*. 14(4): 343–360.