INFORMATION SECURITY CULTURE FOR MALAYSIAN PUBLIC ORGANIZATION: A CONCEPTUAL FRAMEWORK

Mohamad Noorman Masrek[1]*, Qamarul Nazrin Harun[2] and Muhammad Khairulnizan Zaini[3]

[1]Assoc Prof. Dr., Faculty of Information Management, Universiti Teknologi MARA, Shah Alam Selangor, MALAYSIA, mnoormanm@gmail.com
[2] Faculty of Information Management, Universiti Teknologi MARA, Shah Alam Selangor, MALAYSIA, qamarulnaz@gmail.com
[3]Faculty of Information Management, Universiti Teknologi MARA, Shah Alam Selangor, MALAYSIA, nizam0374@salam.uitm.edu.my

*Corresponding Author

Abstract

Information security has traditionally been technology oriented. A survey of the literature shows that research on the technical aspects and formal control of information security is abundant, but emphasizes on social aspects covering employee information security culture has rarely been emphasized. Standards such as GAISP, ISO27002 (or previously known as ISO/BS 17799), SSECMM and Standard of Good Practices have mainly giving emphasize on technical aspects with little attention given on the culture and management of employee information security practices. Given that the employee as the IT users might be a considerable threat to the security level, as well as being essential resources to prevent incidents from happening, non-technological aspects of information security should also be considered in addition to technological aspects. To this effect the need to develop an information security culture (ISC) is crucial so as to protect the organization from any possible information security threats and breaches. ISC can be defined as “information security perceptions, attitudes and assumptions those are accepted and encouraged in an organization – thus the way in which things are done in an organization to protect information assets”. Studies have shown that, when ISC are not in place, employees of the organization will engage in activities that will endanger the well being of the organization, such as accessing and disclosing confidential information, exploiting information resources for personal gains etc. Against this background, an ISC framework for Malaysian Public Sector organizations is proposed. The framework consists of six dimensions, namely, management support, policy and procedures, compliance, awareness, budget and technology. Each of these dimensions is further divided into sub-dimensions. The developed framework will be empirically validated and tested using qualitative and qualitative approach with focus group interview and questionnaire as the data collection technique.

Keywords: information security culture, information security breaches, conceptual framework

1 INTRODUCTION

Information security has traditionally been technology oriented. A survey of the literature shows that research on the technical aspects and formal control of information security is abundant, but emphasizes on social aspects covering employee information security culture has rarely been emphasized. Standards such as GAISP, ISO27002 (or previously known as ISO/BS 17799), SSECMM and Standard of Good Practices have mainly giving emphasize on technical aspects with little attention given on the culture and management of employee information security practices. Given that the employee as the IT users might be a considerable threat to the security level, as well as being essential resources to prevent incidents from happening, non-technological aspects of information security should also be considered in addition to technological aspects. To this effect the need to develop an information security culture (ISC) is crucial so as to protect the organization from any possible information security threats and breaches.

ISC can be defined as "information security perceptions, attitudes and assumptions those are accepted and encouraged in an organization – thus the way in which things are done in an organization to protect information assets" (Da Viega et al., 2007). Studies have shown that, when ISC are not in place, employees of the organization will engage in activities that will endanger the well being of the organization, such as accessing and disclosing confidential information, exploiting information resources for personal gains etc.

The Malaysia's Critical National Information Infrastructure (CNII) places great concern on information security. This is because, theft of information and intellectual property will drive investment away from countries whose systems are seen to be insecure. Against this background, an ISC framework for Malaysian Public Sector organizations is proposed. The framework is expected to facilitate the development of information security culture for Malaysian Public Sector organizations. A culturally secured information security practices, will protect and safeguard government information from any possible threats and leakage. Having a strong and sound information security practices will further boost the confidence of prospective investor to invest in this country.

2 DEVELOPING INFORMATION SECURITY CULTURE

Martins & Eloff (2002) described information security as "a set of information security characteristics that the organization values; the assumption about what is acceptable and what is not in relation to information security; the assumption about what information security behavior is encouraged and what is not; the way people behave towards information security in the organization. If an organization is trying to foster a subculture of information security, all activities would have to be performed in a way that is consistent with good information security practice. Having adequate knowledge regarding information security is a prerequisite to performing any normal activity in a secure manner. According to Schlienger & Teufel (2003), when developing information security culture, the following aspects need to be given attention, namely artifacts, espoused values and shared tacit assumptions.

Artifacts are things or events that happen in the organization. Employees need to be equipped with the necessary skills and competencies to perform security related tasks correctly and securely. Espoused values are concerned with knowing and understanding the information security needs of the organization. The person or team, responsible for the drafting of the information security policy must fully understand the information requirements as needed by their organizations. The shared tacit assumptions are the beliefs and values of employees, which should be in tandem or in sync with espoused values. ISC, similar to organizational culture, can't be created once and then be used all life time. ISC must be created, maintained or changed continuously and the process is iterative and will never end.

3 PROPOSED FRAMEWORK

Figure 1 depicts the theoretical framework of the study. The framework is developed based on the work of Aksu et al. (2015), Alhogail and Mirza (2014), Alnatheer & Nelson (2009), Jacobs (2013), Mark & Michael (2009), Martins & Veiga (2015), Mohamed et al. (2012), Omar (2007), Shaaban (2014), Veiga and Eloff (2007). Information Security Culture (ISC) consists of six dimensions, namely management support, policy and procedures, compliance, awareness, budget and technology. The management support is divided into two sub-dimensions which are information security commitment and information security importance. Policy and procedure dimensions comprised of information security policy effectiveness and information security directives. Compliance dimensions consist of information security monitoring perception and information security consequences. While awareness also composed of two sub-dimensions which are information security responsibility and information security training. Budget dimensions involved information security budget practice and information security investment. Lastly, technology dimensions consist of information

security capability and information security compatibility. An effective and comprehensive ISC would normally result in the prevention and protection of organizational information assets from security breaches. However, when ISC is not proper, information security breaches will tend to take place.

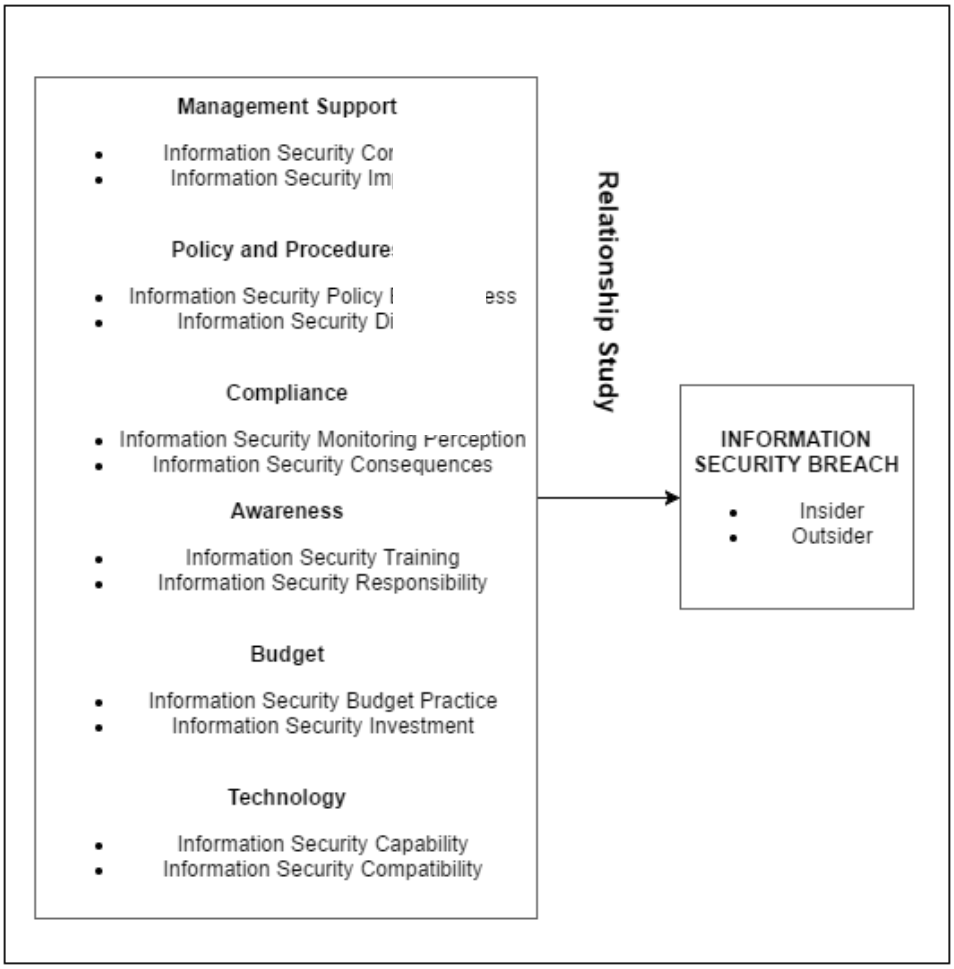

Figure 1. Conceptual Framework

3.1 Internal Information Security Breaches

National Cybersecurity and Communications Integration Centre (NCCIC) of United States of America (2014) has defined insider threat as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems. Infosec Institute (2014) reported that insider threat were considered as one of the most significant risks to the overall security of any organization. From the reported, they revealed that 37% ex-employee had caused fraud towards their former organization, 21% of ex-employees had caused IT sabotage, 19% of ex-employees had espionage the classified information, 15% of employees had caused Intellectual Property (IP) theft incident and 8% are other insider threats.

3.2 Outsider Information Security Breaches

Outsider threats can be defined as Information security breaches or threats that mainly caused by untrusted and unauthorized individuals or group over the organization's information assets (Franqueira et al., 2010). Diaz-Gomez, (2010) added that outsider threats can be classified as external threats outside the organization which interest parties try to access the system. Price Water House Coopers (2015) has reported that outsider threats can be considered as the most dangerous threats that can take down the organization. They also noted that 10% of the outsider threats come from terrorists, 15% are organized crime that intentionally planning on take down the organization, 16% are from activist organizations or hacktivists, 16% of outsider threats are information brokers which violates the organization's security systems in order to gain the confidential information, 24% of the outsider threats comes from their competitors, 9% are from foreign

entities and organizations, 7% are from foreign nation-states, 6% are from domestic intelligence service, 24% of outsider threats are from hackers and 18% of outsider threats are unknown.

3.3 Information Security Commitment

The ISO/IEC 17799 standard (2005) outlines that commitment is a crucial ingredient for the success of information security implementation. Liang et al. (2007) defined information security commitment as the degree to which top management give full supports and show their involvement towards an organizational initiative on information security. Barton (2014) stated that although top management commitment does not guarantee effective operational security, it is a prerequisite for effective development, implementation, and compliance with information security policy. Kajava et al. (2006) opined that commitment is about getting "personally involved" with the information security initiatives. ISACA (2005) identified that senior management's commitment to information security initiatives as the number one critical element impacting an information security program's success. With this justification, the following proposition is established: **P1 – There is a negative relationship between information security commitment and Information security breaches.**

3.4 Information Security Importance

Information security importance can be understood as management commitment in managing information security in an organization that reflect employees behaviour when protecting information security assets from any threats (Zhang et al., 2009). The behavior of the employees is significantly affected by the behavior of their superiors or managers. When the managers themselves demonstrates a behavior that reflects their deep concern and giving significant priority regarding information security, their employees will definitely follow suit. In contrast, a take-for-granted or giving less-attention-behavior by the managers, will also influence employee not to give serious attention regarding the protection of the information security assets. A worldwide survey by CISCO (2008) discovered that the majority of IT professionals believes that employees did not always adhere to policies because security was not a top-of-mind priority or issue. Driven by the aforementioned reason, the following proposition is established: **P2 – There is a negative relationship between information security importance and information security breaches.**

3.5 Information Security Policy Effectiveness

Martins & Veiga (2015) defined information security policy effectiveness as the appraisal of the information security policy, whether its is understandable, practical and successfully communicated. A well-written information security policy should be clear and concise, with easily understandable language and free from any legal and technical jargon. In addition, it must be practical, functional, and enforceable. Because the workplace is constantly changing, policies and procedures relating to information security also change sparingly. Communicating information security policy on a regular basis ensures that employees are well informed. A survey by CISCO (2008) revealed that, "the methods used to communicate information security policies to employees and the perceived fairness of the policies are critical to success". The findings also showed that 40% of employees in the surveyed companies did not know that the security policies existed- and a surprising 20% of IT professionals were unaware of an existing security policy. Given this background, we expect that an effective information security policy will result in reduced information security breaches, Thus, the following proposition is put forward: **P3 – There is a negative relationship between information security policy effectiveness and information security breaches.**

3.6 Information Security Directives

Every organization needs to provide clear directions in protecting their information security assets. Information security directives give light guidance to employees on what procedures need to follow when information security breaches take place. Information security directives can be understood as the clear direction or instruction of protecting information security assets from information security incidents such as information security breaches that caused by unauthorized parties (Mansky et al., 2008). Various studies stated that many organizations suffer from data losses because of clear directives in protecting information security assets were not provided to employees (Ifinedo, 2014; Martins & Veiga, 2010). Based on this rationale, it is proposed that: **P4 – There is a negative relationship between information security directives and Information security breaches.**

3.7 Information Security Monitoring

Information security monitoring perception can be defined as the perception regarding monitoring and disciplinary action (Martins & Veiga, 2015). Employees' misbehaviour can be most crucial factors that cause

information security breaches within organizations (Alhogail & Mirza, 2014; Alkalbani, 2013; Veiga, 2008; Knapp, 2005; Martins & Eloff, 2002; Martins & Veiga, 2015; Martins, 2015; Martins & Veiga, 2010). It shows that information security monitoring perception would be importance element in cultivating ISC which preventing employees from make mistakes when handling information security assets. Thus, the following proposition is formulated: **P5 – There is a negative relationship between information security monitoring and Information security breaches.**

3.8 Information Security Consequences

Volkamer et al. (2013) stated that information security consequences happen when an attacker gets access to private data (e.g. confidential report, history, salary, photos, and email history), losing money, and different types of a nuisance that give negative effects to the organization Moreover, information security consequences can be understood as the necessary action need to be taken by management when the organization need to deal with any non-compliance events (Mohamed et al., 2012). Previous studies found that information security consequences could be importance element in implement ISC (Musa, 2010; Veiga, 2016) Organizations that effectively take necessary actions when information security breaches occur will reduce the chances recurrence. In line with this justification, the following preposition is established: **P6 – There is a negative relationship between information security consequences and Information security breaches**.

3.9 Information Security Responsibilities

In information security context, management and employees have equal responsibilities to prevent, protect, safeguard information assets. Lim et al., (2010) defined information security responsibilities as the person or department consists of small group of people that is responsible for ensuring the compliance of information security policies. Previous studies revealed that employee that put full responsibility towards their work tasks have higher motivation and loyalty which influence the organization's productivity in managing information security assets (Alkalbani et al., 2015; Alnatheer, 2012; Martins & Eloff, 2001; Martins & Eloff, 2002; Martins & Veiga, 2015). In Malaysian public organization environment, the IT department is responsible in managing information security assets. With this justification, the researcher established that: **P7 – There is a negative relationship between information security responsibilities and Information security breaches.**

3.10 Information Security Training

Most organizations provide training for their employees as a tool to boost their productivity by upgrading employees' skills and knowledge. Information security training can be effective tools in order to prepare the employees in protecting information security assets by improving their capabilities in managing information security assets within organizations. Martins & Veiga (2015) indicated that information security training is established to enable employees to protect themselves, create knowledge in terms of finding, understanding and using information security assets in organizations. Past studies have shown that information security training has positive factors that can influence employees in establishing ISC in organizations (Alnatheer, 2015; Veiga & Martins, 2015). Omar (2007) discovereed that, information security training within Malaysian public organization was seen as inadequate by the employees. Without proper and up to date training, employees cannot be able to embrace information security practices and guidelines into their everyday behaviour (Omar, 2007). Accordingly the following preposition is established: **P8 – There is a negative relationship between information security training and Information security breaches.**

3.11 Information Security Budget Practice

According to Lim et al., (2009), information security budget practice can be defined when management in an organization allocates budgets for information security activities annually and acts promptly towards expenses pertaining information security activities and for IT support. Besides that, National Advisory Council on State and Local Budgeting (1998) suggested the definition of budget practice as procedure that assist in accomplishing a principle and element of the budget process. In other word, budget practice is a process that assists management in achieving information security goals which is reducing Information security breaches by allocating specific budget towards information security activities within the organization. Previous studies have showed that information security budget practice gives strong impact on organization's productivity (Dlamini et al., 2011; Kassim & Abdullah, 2006; Veseli, 2011). Organization that allocate budgets in information security activities seem like having more tendency on preventing their information security assets and resources from information security breaches. Therefore, the following preposition is formulated: **P9 – There is a negative relationship between information security budget practice and Information security breaches**.

3.12 Information Security Investment

Toivanen (2015) defined information security investment as a process of investing something to gain something in return which can be seen in the form of capital, time and benefits that could be tangible and intangible. Therefore, any action that has been made by the organization in order to gain something which can be capital, time and benefits in return which support organization's goal can considered as an investment. In order to achieve the organization's goal, employees are responsible to prevent information security assets from any possible threats coming from inside and outside the organization. Thus, by improving employees' awareness and knowledge towards information security threats by sending them to particular training and program can be considered as information security investment. Previous studies have found that the more organization invest their annual budget for information security activities, the lower chances of ISBes occurrence (Ahmad & Maynard, 2013; Alavi et al., 2015; Monfelt et al., 2014; Norshima & Balakrishnan, 2015; Paulsen et al., 2011). Thus, the preposition is established: **P10 – There is a negative relationship between information security investment and Information security breaches**.

3.13 Information Security Capability

Information security capability refers to the ability to fulfil technical security requirements and assists organizations to fulfil information security policy requirements (Alkalbani, 2014). Information security capability can also be referred as the ability to fulfil technical security requirements (Tudir, 2010). Previous studies showed that information security capability encompasses the technology aspects of information security, such as configuring a secure firewall, network and database and also includes business continuity and disaster recovery (Veiga, 2008) and could influence the way information security assets are conducted (Ali, 2014; Alnatheer & Nelson, 2009; Martins & Eloff, 2001; Mohamed et al., 2012). In line with this justification, the following preposition is established: **P11 – There is a negative relationship between information security capability and Information security breaches.**

3.14 Information Security Compatibility

Smetters & Grinter (2002) defined the information security technology compatibility as the technological equipment that has the ability in protecting the information security technologies in order to enforce the security requirements over operational technologies. In addition, information security technological compatibility can be understood as the ability of software and hardware to work together adhering common technology standards (Alkalbani, 2014). Various studies showed that information security technology compatibility is one of significant element that influencing the adoption of ISC within organization (Alkalbani, 2013, 2014; Knapp, 2005; Shaw, 2012). Therefore organizations are recommended to establish information security compatibility within technological equipment in the organization as an effort to minimize information security breaches. Driven by the aforementioned reason, the following proposition is established: **P12 – There is a negative relationship between information security compatibility and Information security breaches.**

4 CONCLUSION

The aim of this paper is to present a proposed conceptual framework for the development of information security culture for the Malaysian public organization. Adopting the literature review approach, a conceptual framework of information security culture is proposed which has six dimensions, namely, management support, policy and procedures, compliance, awareness, budget and technology. Each of these dimensions is further divided into sub-dimensions. The developed framework will be empirically validated and tested using qualitative and qualitative approach with focus group interview and questionnaire as the data collection technique.

ACKOWLEDGEMENT

The researcher would like to extend our thanks and appreciation to Universiti Teknologi MARA (UiTM) and the Ministry of Higher Education (MoHE) Malaysia for funding the project under the Fundamental Research Grant Scheme, file no: FRGS/1/2016/SS09/UITM/02/2.

REFERENCE LIST

Abu-Musa, A. (2010). Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security*, *18*(4), 226–276. Https://doi.org/10.1108/09685221011079180

Ahlan, A. R. (2011). Information Security Awareness in University : Maintaining Learnability , Performance and Adaptability through Roles of Responsibility, 246–250.

Ahmad, A., & Maynard, S. B. (2013). Information Security Management : Factors that Influence Security Investments in SMES.

Aksu, P. K., Kitapçi, N. Şi., & Çatar, R. Ö. (2015). An Evaluation of Information Security from the Users ' Perspective in Turkey, *9*(2), 55–67.

Alavi, R., Islam, S., Mouratidis, H., & Lee, S. (2015). Managing Social Engineering Attacks- Considering Human Factors and Security Investment. *Ninth International Symposium on Human Aspects of Information Security {&} Assurance, {HAISA} 2015 ,Lesvos, Greece, July 1-3, 2015, Proceedings.*, (August 2015), 161–171. Https://doi.org/10.13140/RG.2.1.3646.6408

Alhogail, A., & Mirza, A. (2014a). A Proposal of an Organizational Information Security Culture Framework, 243–250.

Alhogail, A., & Mirza, A. (2014b). Information Security Culture: A Definition and a Literature review. *Computer Applications and Information Systems (WCCCAIS)*, 1–7. Https://doi.org/10.1109/WCCAIS.2014.6916579

Ali, A. (2014). The Effect of Information Technology Capabilities in Implementing , Information Security Management Systems, *10*(18), 377–386.

Alkalbani, A. (2013). Investigating the Role of Socio-organizational Factors in the Information Security Compliance in Organizations, (2010).

Alkalbani, A. (2014). A Conceptual Framework for Information Security in Public Organizations for E-Government Development, (2010).

Alkalbani, A., Deng, H., & Kam, B. (2015). Organisational Security Culture And Information Security Compliance For E-Government Development : The Moderating Effect Of Social.

Alnatheer, M. A. (2012). Understanding and Measuring Information Security Culture in Developing Countries : Case of Saudi Arabia.

Alnatheer, M. A. (2015). Information Security Culture Critical Success Factors. *2015 12th International Conference on Information Technology - New Generations*, 731–735. Https://doi.org/10.1109/ITNG.2015.124

Alnatheer, M., & Nelson, K. (2009). Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context, (December).

Anderson, B. B., Kirwan, C. B., & Eargle, D. (2013). Using Measures of Risk Perception to Predict Information Security Behavior : Insights from Using Measures of Risk Perception to Predict Information Security Behavior : Insights from, *15*(April 2013), 679–722.

Bartlomiej, T. (2014). The Impact Of Information Security Awareness On Compliance With Information Security Policies : A Phishing Perspective Bartlomiej T. Hanus Dissertation Prepared for the Degree of DOCTOR OF PHILOSOPHY August 2014 Approved: John Windsor, Major Professor.

Barton, K. A. (2014). Information System Security Commitment : A Study of External Influences on Senior Management, (19).

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance : The motivators and barriers of employees ' security behaviors. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 103–122.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2006). Role of Perceived Importance of Information Security: An Exploratory Study of Middle School Childrens Information Security Behavior. *Issues in Informing Science and Information Technology*, *3*(2005), 127–135.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers and Security*, *39*(PART B), 447–459. Https://doi.org/10.1016/j.cose.2013.09.009

CISCO. (2008). Corporate Social Responsibility Report.

Critical National Information Infrastructure. (n.d.). Retrieved November 15, 2016, from http://cnii.cybersecurity.my/main/about.html

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Inf. & Comput. Security*, *24*(2), 139–151. Https://doi.org/10.1108/ICS-12-2015-0048

Da Veiga, A. (2008). Cultivating and Assessing Information Security Culture, (September).

Da Veiga, A., & Martins, N. (2015). Information Security Culture: A Comparative Analysis of Four Assessments, 49–57.

Diaz-Gomez, P. (2010). Internal Vs. External Penetrations: A Computer Security Dilemma. *Proceedings of the 2010 International Conference on Security & Management*. Retrieved from http://weblidi.info.unlp.edu.ar/worldcomp2011-mirror/SAM3049.pdf

Dlamini, M. T., Eloff, M. M., Eloff, J. H. P., & Venter, H. S. (2011). A Budget Model for Information Security, (Haisa), 47–57.

Dodge, R., Toregas, C., & Hoffman, L. (2011). Cybersecurity Workforce Development Directions. *Human Aspects of Information Security*, (Haisa), 1–12.

Eccles, D. W., & Feltovich, P. J. (2008). Implications of Domain-General “Psychological Support Skills” for Transfer of Skill and Acquisition of Expertise. *Performance Improvement Quarterly*, *21*(2), 43–60. Https://doi.org/10.1002/piq

Effectiveness, S. (2011). Impact of Security Awareness Training Components on Perceived Security Effectiveness, *4*, 1–6.

Ehmann, E., Houlden, N., & Grout, V. (2012). Using Complex Adaptive Systems and Technology to Analyse the Strength of Processes and Cultural Indicators : A Method to Improve Sustained Competitive, 139–147.

Feller, J., Finnegan, P., Hayes, J., & O’Reilly, P. (2009). Institutionalising information asymmetry: governance structures for open innovation. *Information Technology People*, *22*(4), 297–316. Https://doi.org/10.1108/09593840911002423

Frangopoulos, E. D., Eloff, M. M., & Venter, L. M. (2014). Human Aspects of Information Assurance : A Questionnaire-based Quantitative Approach to Assessment, (Haisa), 217–229.

Franqueira, V. N. L., Van Cleeff, A., Van Eck, P., & Wieringa, R. (2010). External insider threat: A real security challenge in enterprise value webs. *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, 446–453. Https://doi.org/10.1109/ARES.2010.40

Helkala, K., & Bakås, T. H. (2013). National Password Security Survey : Results, (Eismc), 23–33.

Hennie, K., Lynette, D., & Tjaart, S. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, *18*(5), 316–327. Https://doi.org/10.1108/09685221011095236

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations : Role of penalties , pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. Https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, *18*(2), 106–125. Https://doi.org/10.1057/ejis.2009.6

Humaidi, N., & Balakrishnan, V. (2013). Informatics Exploratory Factor Analysis of User ’ s Compliance Behaviour towards Health Information System ’ s Security, *4*(2), 2–9. Https://doi.org/10.4172/2157-7420.1000123

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79. Https://doi.org/10.1016/j.im.2013.10.001

Institute, I. (2014). *2013 Data Breaches: All You Need to Know*. Retrieved from http://resources.infosecinstitute.com/2013-data-breaches-need-know/

ISACA. (2005). IS Audit and Assurance Guideline 2204 Materiality IS Audit and Assurance Guideline 2204 Materiality The guideline is presented in the following sections : 1 . Guideline Purpose and Linkage to Standards.

Jacobs, G. (2013). A theoretical framework of organizational change, (241918). Https://doi.org/10.1108/JOCM-09-2012-0137

Kajava, J., Kajava, J., Varonen, R., & Roning, J. (2006). Senior Executives Commitment to Information Security - from Motivation to Responsibility University of Lapland Reijo Savola VTT Technical Research Centre of Finland, 1519–1522.

Kam, H., Katerrattanakul, P., Gogolin, G., & Hong, S. (2013). Information Security Policy Compliance in Higher Education: a Neo-Institutional Perspective. *PACIS 2013 Proceedings*, Paper 106.

Kargbo, J. A. . (2009). Automation: Whither Academic Libraries? View From Practice. *Information Technology for Development*, *15*(1), 43–51. Https://doi.org/10.1002/itdj

Kassim, N. M., & Abdulla, A. K. M. A. (2006). The influence of attraction on internet banking: an extension to the trust-relationship commitment model. *International Journal of Bank Marketing*, *24*(6), 424–442. Https://doi.org/10.1108/02652320610701744

Knapp, K. J. (2005). A Model Of Managerial Effectiveness In Information Security : From Grounded Theory To Empirical Test Submitted to The Graduate Faculty of Auburn University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy Auburn , Alabama.

Lee, H.-A., Mat Zin, R., & PM Dato' Seri Abdullah Ahmad Badawi. (2014). Malaysian Development Experience : Lessons for Developing Countries. *Institutions and Economies*, *6*(1), 65–81. Retrieved from https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/data-breach-notification.pdf

Li, Y. (2015). *Users' information systems (IS) security behavior in different contexts*.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management.

Lif, P., & Sommestad, T. (2015). Human factors related to the performance of intrusion detection operators. *Human Aspects of Information Security, Privacy, and Trust*, (Haisa), 265–275.

Lim, J., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the relationship between organizational culture and information security culture. *Proceedings of the 7th Australian Information Security Management Conference*, (December), 88–97. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?Article=1011&context=ism

Lim, J. S., Ahmad, A., Chang, S., & Maynard, S. (2010). Embedding Information Security Culture, 463–474.

Lim, J. S. J., Chang, S., Maynard, S., Ahmad, A., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the relationship between organizational culture and information security culture. *Proceedings of the 7th Australian Information Security Management Conference*, (December), 88–97. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?Article=1011&context=ism

Mansky, B., Milne, K., Swanson, D., & Violago, D. (2008). Assessment of Information Security Awareness June 2008, (June).

Mark, B., & Michael, J. (2009). An Integrated Framework for Information Security Management.

Martins, A., & Eloff, J. (2002). Information Security Culture. *Security in the Information Society*, 203–214. Https://doi.org/10.1007/978-0-387-35586-3_16

Martins, A., & Eloff, J. H. P. (2001). Information System Security Attribute Quantification or Ordering. *Workshop on Information Security System Scoring and Ranking*, 70.

Martins, N. (2015a). Improving the information security culture through monitoring and implementation actions illustrated through a case study, *9*. Https://doi.org/10.1016/j.cose.2014.12.006

Martins, N. (2015b). Information security culture and information protection culture : A validated assessment instrument, *1*. Https://doi.org/10.1016/j.clsr.2015.01.005

Martins, N., & Veiga, A. (2010). The Value of Using a Validated Information Security Culture Assessment Instrument, 146–154.

Martins, N., & Veiga, A. Da. (2015). An Information Security Culture Model Validated with Structural Equation Modelling, (Haisa), 11–21.

Meske, D. J. (2011). Data Loss : Protecting Personally Identifying Information (PII) at Public Higher Education Institutions, (August).

Moag, J., & Johnson, M. E. (2011). *Human Behavior and Security Culture*.

Mo Ismail. (2014). User Compliance to Information Security Policy.

Mohamed, N., a/p Gian Singh, J. K., Norshidah Mohamed, & Jasber Kaur a/p Gian Singh. (2012). A conceptual framework for information technology governance effectiveness in private organizations. *Information Management & Computer Security*, *20*(2), 88–106. Https://doi.org/10.1108/09685221211235616

Molla, A., & Licker, P. S. (2005). Ecommerce adoption in developing countries: A model and instrument. *Information and Management*, *42*(6), 877–899. Https://doi.org/10.1016/j.im.2004.09.002

Monfelt, Y., Pilemalm, S., Hallberg, J., & Yngstrom, L. (2014). The 14-layered framework for including social and organizational aspects in security management. Https://doi.org/10.1108/09685221111143060

Moynihan, D. P. (2004). Building secure elections: E-voting, security, and systems theory. *Public Administration Review*, *64*(5), 515–528. Https://doi.org/10.1111/j.1540-6210.2004.00400.x

Muda, M. Z. Bin. (2010). Awareness and Acceptance Analysis of Information Security Policy, (March).

Muhire, B. (2012). Employee Compliance with Information Systems Security Policy in Retail Industry . Case : Store Level Employees Employee Compliance with Infor- mation Systems Security Policy in Re- tail Industry . Case : Store Level Em- ployees Honors Thesis Bertrand Muhi.

National Advisory Council on State and Local Budgeting. (1998). *Recommended Budget Practices:A Framework For Improved State and Local Government Budgeting*. Retrieved from http://www.gfoa.org/services/dfl/budget/recommendedbudgetpractices.pdf

NCCIC. (2014). Combating the Insider Threat. *National Cybersecurity and Communications Integration Center*, (May), 61–64. Retrieved from https://www.us-cert.gov/sites/default/files/publications/Combating the Insider Threat_0.pdf

Norshima Humaidi, & Balakrishnan, V. (2015). The Moderating Effect Of Working Experience On Health Information System, *28*(2), 70–92.

Omar, Z. (2007). Investigating information security culture in a public sector organisation : challenges Malaysian a case, (June).

Parsons, K., Mccormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. Https://doi.org/10.1016/j.cose.2013.12.003

Patel, A., Qassim, Q., Shukor, Z., Nogueira, J. H. M., Júnior, J. C., & Wills, C. (2010). Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System. *Proceeding of the South African Information Security Multi-Conference (SAISM 2010)*, (Saismc), 223–234.

Paulsen, C., Student, G., & Coulson, T. (2011). Beyond Awareness : Using Business Intelligence to Create a Culture of Information Security, *11*(3), 35–54.

Pierce, R. E. (2012). Key Factors In The Success Of An Organization ' S Information Security Culture : A Quantitative Study And Analysis By Robert E . Pierce Edward M . Goldberg, D. M., Committee Member MARK C . BANNISTER , J. D., Committee Member William A . Reed , Ph ., (October).

Pricewaterhousecoopers International Limited. (2015). *Managing cyber risks in an interconnected world*.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education : An exploratory study. *Computers & Security*, *27*(7–8), 241–253. Https://doi.org/10.1016/j.cose.2008.07.008

Ruxwana, N., Herselman, M., & Pottas, D. (2010). Community awareness and involvement: An overlooked security control. *Proceedings of the South African Information Security Multi-Conference, SAISMC 2010*, (Saismc), 47–60. Retrieved from http://www.scopus.com/inward/record.url?Eid=2-s2.0-84926214918&partnerid=tzotx3y1

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: Increased trust by an appropriate information security culture. *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA*, *2003–Janua*, 405–409. Https://doi.org/10.1109/DEXA.2003.1232055

Shaaban, H. K. (2014). Enhancing The Governance Of Information Security In Developing Countries: The Case Of Zanzibar by Shafiu, I. (2015). Information Security Compliance Behaviour in Supply Chain Security.

Smetters, D. K., & Grinter, R. E. (2002). Moving from the design of usable security technologies to the design of useful secure applications. *Proceedings of the 2002 Workshop on New Security Paradigms - NSPW '02*, 82. Https://doi.org/10.1145/844115.844117

Smith, S., & Jamieson, R. (2006). Determining Key Factors in E-Government Information System Security. *Information Systems Management*, *23*(2), 23–32. Https://doi.org/10.1201/1078.10580530/45925.23.2.20060301/92671.4

Thomson, K., & Niekerk, J. Van. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*, *20*(1), 39–46. Https://doi.org/10.1108/09685221211219191

Thurlby, C., Langensiepen, C., Haggerty, J., & Ranson, R. (2015). Understanding User Knowledge of Computer Security and Risk : A Comparative Study, (Haisa), 194–203.

Toivanen, H. (2015). Case Study of Why Information Security Investment Decision Fail ?

Topa, I., & Karyda, M. (2015). Trust, Privacy and Security in Digital Business: 12th International Conference, trustbus 2015 Valencia, Spain, September 1-2, 2015 Proceedings. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9264*(September), 5. Https://doi.org/10.1007/978-3-319-22906-5

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., & Gritzalis, S. (2010). Unifying ISO Security Standards Practices into a Single Security Framework, (Saismc), 188–203.

Valjarevic, A., & Venter, H. (2012). Towards Solving the Identity Challenge. *The 7th International Workshop on Digital Forensics and Incident Analysis (WDFIA 2012)*, (Wdfia), 129–138.

Veiga, A. Da, & Eloff, J. H. P. (2007). An Information Security Governance Framework.

Venter, H., & Karie, N. M. (2013). An Ontological Framework for a Cloud Forensic Environment. *Proceedings of the European Information Security Multi-Conference (EISMC 2013)*, (Eismc), 112–122.

Veseli, I. (2011). Measuring the Effectiveness of Information Security Awareness Program.

Volkamer, M., Bartsch, S., & Kauer, M. (2013). Contextualized security interventions in password transmission scenarios. *Proceedings of the European Information Security Multi-Conference, EISMC 2013*, (Eismc), 12–22. Retrieved from http://www.scopus.com/inward/record.url?Eid=2-s2.0-84926145504&partnerid=tzotx3y1

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330–340. Https://doi.org/10.1108/09685220910993980