AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Determining critical success factors (CSF) of information security knowledge (ISK) towards organisations' information security effectiveness

[1]Rohana Mohamad Rashid, [2]Omar Zakaria, [3]Nabil Zulhemay

[1,2,3]*National Defence University of Malaysia, Faculty of Defence Science and Technology, 57000 Kuala Lumpur, Malaysia.*

ARTICLE INFO

Article history:
Received 30 September 2014
Received in revised form
17 November 2014
Accepted 25 November 2014
Available online 6 December 2014

Keywords:
human factor, information security, information security effectiveness, knowledge, knowledge management

ABSTRACT

Background: The increasingly of internal security incidents that mostly caused by human factor nowadays is deeply disturbing and give the bad impact to the organisations' information security effectiveness. Therefore, this study is to investigate the critical success factors of information security knowledge (ISK) that have the significance impact to the organisations' information security effectiveness among Malaysian public sector organisation. Through literature, there are five critical success factors (knowledge, employee behaviour, knowledge sharing, protection of information, and motivation) that have the significance impact to the organisations' information security effectiveness and one factor (leadership) that have been identify as moderator towards achieving organisations' effectiveness. This research adapts quantitative research method (questionnaire survey). SPSS 16.0 and SmartPLS 2.0 software used to analyse data and verify hypotheses.

ToCite ThisArticle: Rohana Mohamad Rashid, Omar Zakaria, Nabil Zulhemay., Determining critical success factors (CSF) of information security knowledge (ISK) towards organisations' information security effectiveness. ***Aust. J. Basic & Appl. Sci.,*** *8(23): 336-344, 2014*

INTRODUCTION

Today, knowledge is considered as the main key for competitiveness among organisations. As IT Governance Institute (2006) underscores, in order to achieve effectiveness in today's complex interconnected world, information security must be addressed at the highest level of the organisation. The rapid growth of technology has caused many organisation deals with such device of technology in order to ensure that they keep abreast of current technology. As more organisations get connected and invest into IT, the security concerns will grow and new threats will emerge, thus making organisation vulnerable. Insufficient attention to human factors in system design and implementation for ICT outsourcing project contribute to the most of information security issues that probably influence other security risk factors (Khidzir, Mohamed, & Arshad, 2010). Here, information security knowledge (ISK) is introduces which may guide employees in implementing information security practices within the organisation. Having ISK in organisation may help decrease the internal security incidents that are posed by humans hence will lead to the organisational information security effectiveness.

The objective of this study is to identify the critical success factors that enable employees to adopt ISK in their organisation in order to achieve organisations' information security effectiveness. To achieve the objective of the study, an integrated conceptual framework has been proposed and validated which is based on human factors perspectives.

Literature Review:

The Definition of Information Security:

Security is the process of reducing risks or threats that can jeopardise an organisation, meanwhile information security is a business requirement to protect the organisation's investment in its information assets (Pipkin, 2000). The Information Security Management System (ISMS) defines information security as a preservation of confidentiality, integrity, and availability of information; in addition with other properties such as authenticity, accountability, non-repudiation and reliability (Cyber Security Malaysia, 2010). The other definition is from the Committee on National Security System (CNSS) where they define information security as the protection of information and its critical elements (hardware and software) (Whitman &Mattord, 2012). These two definition is compatible with the purpose of information security to protect and preserve the confidentiality, integrity, and availability of information that may also involve protecting and preserving the

Corresponding Author: Rohana Mohamad Rashid, National Defence University Of Malaysia, Faculty of Defense Science and Technology, 57000 Kuala Lumpur, Malaysia.
E-mail: rohana.mrashid@gmail.com

authenticity and reliability of information and ensuring that entities can be held accountable (ISO IEC 27000 2014, 2014).

The Definition of Knowledge And Knowledge Management:

Although knowledge is derived from information, knowledge also can become information. This is explained by Alavi and Leidner (2001) where they state that information is converted into knowledge once it is processed in an individual's mind and knowledge becomes information once it is articulated and presented in the form of text, words, graphics, or other symbolic forms. This implies that knowledge can become information when it is stored in documents, books, policies, procedures, computers, or other repositories, but then becomes knowledge again when it is transferred to another human (Hicks, Dattero, & Galup, 2006).

The term 'knowledge management' is used to describe everything starting from the application of new technology to the achievement in intellectual capital of an organisation (Sallis & Jones, 2002). All organisation use and generate knowledge. Then, combining knowledge with some values, strategies, and experiences, a good decision can be made. The role of knowledge management is really important to manage the knowledge of information security as the definition of knowledge management is "the capability by which communities capture the knowledge that is critical to their success, constantly improve it, and make it available in the most effective manner to those who need it" (Birkenkrahe, 2002).

Introduction of Information Security Knowledge (ISK):

The relationship of information security, knowledge, and knowledge management is encompassed by the term 'information security knowledge (ISK)'. Defining ISK includes combining all related elements in information security, knowledge, and knowledge management. Table 1 specifies the element of ISK that are extracted from the elements in information security, knowledge management, and knowledge.

Table 1: Information security knowledge's (ISK) elements

Field	Elements
Information security	Protection, confidentiality, integrity, availability (CIA)
Knowledge management	Knowledge sharing, learning, practice
Knowledge	Information, value, experience, insight
Information security knowledge (ISK)	Protection, confidentiality, integrity, availability (CIA), knowledge sharing, learning, practice, information, value, experience, insight

ISK can be defined as the experience, values, and contextual information from the awareness, training and education programme and is learned, shared and practiced by users in their daily work routines towards the protection of information. Applying ISK can significantly impact the effectiveness of information security in organisation and at the same time reduces the security threats.

Everyone in organisation must have the knowledge on information security because it is very important to protect organisation assets and prevent the security incident. But not all users would need to have the same knowledge or education because each category of users is different. According to Niekerk (2005), there are three categories of users that need to be educated in term of information security which are the End Users, IT Personnel, and Top Management. And all these categories of users have different knowledge and education that based on their responsibility and their work. Table 1 shows the users with the minimal knowledge needed.

Table 2: Users categories with minimal knowledge needed

Categories of Users	Minimal Knowledge Needed
The End Users	✓ Knowledge on training and password management for example how to create a strong password. ✓ Knowledge on computer viruses and the safe usage of email
IT Personnel	✓ Knowledge and education on information security technical controls
Top Management	✓ Also need to have knowledge and education on user's training ✓ Knowledge and education on information security policy, procedures, and controls in organisation. ✓ Knowledge to make decision making.

Based on Table 2 we can see that there are different users with different knowledge, therefore it is encourage to share the knowledge to others because information security knowledge must be shared, learned, and practiced to make sure that all users in organisation know what ISK is and can practice the knowledge in organisation. Therefore, by adapting one of knowledge creation that proposed by Nonaka (1995), which is externalisation process can cultivate a good culture in sharing, learning, and performing the information security knowledge in a right way. Shuangyan, Chinghang, and Lamfor (2006)assert that ISK is one of the main important in sustaining good information security in organisation. For the beginning, organisation should have awareness in protecting the information assets in organisation. Hence, by understanding ISK and practice it may

reduce some internal security incidents that mostly cause by human. At the same time, having information security awareness on the importance of information security can be nurtured.

It is important to have ISK since nowadays there are too many security incidents occurs in organisation that will give the bad impact on organisation. Security incidents that occur in an organisation are mostly caused by internal and external security threats. However, this research will focus on internal security threats in organisation. Internal security threat is threat that involve a broad range of events, incidents, and attack that caused by the company's own staff, which means its authorised IT users (Leach, 2003). According to Durgin (2007), an internal security threat occurs when a resource inside the organisation is used in the attack. For example the employee that using the anonymity of the Internet to cover their tracks, to an outside entity that unknowingly factors into the execution of a security incidents. Other than employee, contractor or third party support technician who runs software or makes a change that has a negative impact on the organisation could be the resource of internal threats in an organisation.

In order to find the gaps between this research and previous research on the issues of information security knowledge, a review on previous researches on related topic is discusses in the next section. Besides, with the review on previous work will provides a framework for establishing the importance of the research as well as benchmark for comparing the results with other findings. Also, with the review of previous researches, the variables can be verified.

Previous research on ISK:

Prior research has recognised that technological and organisational factors are not the only key to the organisations' information security effectiveness, there is also need to understand the impact of human factors, moreover, when the issues of ISK have been highlighted. In technological issues, ISK can be verifying through the knowledge and experience in information security concept, operating system, application systems or can be measured through information security certification for example Microsoft and Cisco or more advance certification for example COMPTIA certification. As research done by Grillo (2008), he examine ISK and vulnerabilities at Alamo Community College District by using test scores from COMPTIA Security+ examination.

In organisational issues, Kankanhalli, Teo, Tan, and Wei (2003) find out that organisation size, top management support, and industry type influence the information security in organisation which lead to enhance IS security effectiveness. They also develop a model of IS security effectiveness that incorporates organisational factors. They insert the element of knowledge in their research by proposing to organisation to hire educated and well trained employee that may improves the organisations' performance.

Even though there are researchers (Boonmak, 2008; Niekerk, 2005; Nikolakopoulos, 2009; Parsons, McCormac, Butavicius, & Ferguson, 2010; Risvold, 2010) that study the human factors issues on information security, all the research did not include the study on ISK in human factors except for Niekerk (2005). Niekerk (2005)studies on the information security culture in organisation using education approach. In his study, he asserts that human factors in information security constituted by behaviour and knowledge because humans involved in the security process. Besides, human also need to use their knowledge in carrying out their duties and responsible. Therefore, they have to be educated to perform their job. Hence, he stresses that it is important to have an information security education programme to teach employees the requisite knowledge. Although he relates knowledge on information security and attitude of employees with human factors, he did not study the impact of ISK on human factors. Therefore, this research tries to dig up the issues on ISK on human factors towards organisations' information security effectiveness because little, or no, knowledge exist on how ISK affects organisations' information security effectiveness.

Table 3: Past study on Human Factor in Information Security Related

	Human Factor	Source
1.	Knowledge	Belsis, Kokolakis, and Kiountouzis (2005); Zakaria (2006); Thomson and Von Solms (2006); Jennex and Zyngier (2007);Albrechtsen (2007); Alfawaz, Nelson, and Mohannak (2010); Mittal, Roy, and Saxena (2010b); Ping (2010); Siu and Hui (2011); Babatunde and Selamat (2011);Kuo, Chi, and Dorjgotov (2011); Hennie, Lynette, and Tjaart (2010).
2.	Behaviour	Nosworthy (2000); Goh (2003); Leach (2003); Thomson, Von Solms, and Louw (2006); Albrechtsen (2007); Okunoye and Bertaux (2008); Colwill (2009); Lim, Chang, Maynard, and Ahmad (2009); Alfawaz *et al*. (2010); Babatunde and Selamat (2011); Huang, Rau, and Salvendy (2007); Herath and Rao (2009).
3.	Motivation and Commitment	Leach (2003); Zakaria (2006); Albrechtsen (2007); Lim *et al*. (2009); Mittal *et al*. (2010b); Sandhu, Jain, and Ahmad (2011); Babatunde and Selamat (2011); Danish and Usman (2010); Malik and Ghafoor (2011)
4.	Knowledge Sharing	Nosworthy (2000); (Zakaria (2006), 2007)); Jennex and Zyngier (2007);(Mittal, Roy, and Saxena (2010a); Mittal *et al*. (2010b)); Sandhu *et al*. (2011); Jen-Te (2007); Du, Ai, and Ren (2007)
5.	Protection of Information	Nosworthy (2000); Kankanhalli *et al*. (2003); Belsis *et al*. (2005); (Zakaria (2006), 2007)); Jennex and Zyngier (2007); Albrechtsen (2007); Okunoye and

		Bertaux (2008); Colwill (2009); Babatunde and Selamat (2011); Kwo-Shing, Yen-Ping, Louis, and Jih-Hsing (2006).

Based on the literature on the related area, theory, and empirical evidence, the critical success factors of ISK are knowledge, behaviour, motivation, knowledge sharing, and protection of information (see Table 3). All these factors are clarified as the factors that may influence the organisations' information security effectiveness. Therefore, all these elements are identified as independent variables.

The Critical Success Factors of ISK:

Past studies have identified the critical success factors of ISK from the various sources. Therefore, it is important to highlight the operational definition of each factor. Table 4 shows the definition of each factor of ISK.

Table 4: The Operational Definition of Critical Success Factors of ISK

Factors	Operational definition	Source
Knowledge	Knowledge is a fluid mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences and information.	Davenport and Prusak (1998)
Employee behaviour	Behaviour can be defined as the way in which one acts or conducts oneself, especially towards others; the way in which an animal or a person behaves in response to a particular situation or stimulus; the way in which a machines or natural phenomenon works or functions Adapting the definition of behaviour in employee behaviour in organisation, employee behaviour can be defined as the way of employee behaves in doing their work either in positive way or in negative way. The employee behaviour in organisation may affect the organisations' information security effectiveness.	Oxford Dictionaries (2012a)
Motivation	A reason or reasons for acting or behaving in a particular way. An encouragement and direction to behaviour to achieve goals. In organisational context, motivation can be defines as a reason for engaging in a particular behaviour, especially employee behaviour towards achieving organisation's goals and objective.	Oxford Dictionaries (2012b), Bartol and Martin (1998)
Knowledge sharing	An activity of transferring or disseminating knowledge from one person, group, or organisation, to another. The transfer of valuable facts, belief, perspectives, concepts learned through study, observation or personal experience from knower to knowee.	Lee (2001), Sandhu *et al*. (2011)
Protection of information	The action of protecting someone or something, or the state of being protected. In information security, the protection of information includes the entire set of controls and safeguards, including policy, education, training and awareness, and technology, that implements by organisation in order to protect the assets	Whitman and Mattord (2012)
Leadership	The exercise of command, direction, and control by a leader over an organisation and its members". Many scholars define leadership is the process of influencing, encouraging and helping others to work enthusiastically and to understand and agree about what needs to be done and how it can be done effectively in order to achieve the objectives	*Dictionary of Business and Management* 1999), Higgins (1998), Wirtz and Lwin (2009), Higgins, Shah, and Friedman (1997)

Research Framework:

As mentioned before, the objective of this research is to determine the critical success factors of ISK among public sector organisations in Malaysia. Based on literature review, there are five critical success factors of ISK that have been identified: knowledge; employee behaviour; knowledge sharing; protection of information, and motivation. Leadership is identified as moderator variable in this study. Figure 1 shows the diagram of the proposed framework.

Australian Journal of Basic and Applied Sciences, 8(23) Special 2014, Pages: 336-344

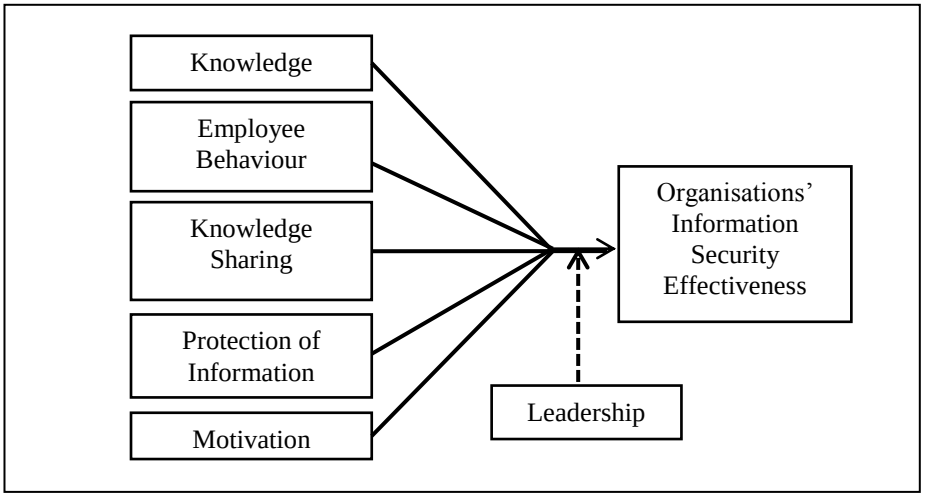

Fig. 1: The Proposed Framework for Critical Success Factors of ISK

The list of constructs and summaries of hypotheses are presented in Table 5. This study has eleven hypotheses which are:

H1: There is a positive relationship between knowledge and organisations' information security effectiveness
H1a: Leadership is moderate the relationship between knowledge and organisations' information security effectiveness

H2: There is a positive relationship between employee behaviour and organisations' information security effectiveness
H2a: Leadership is moderate the relationship between employee behaviour and organisations' information security effectiveness

H3: There is a positive relationship between knowledge sharing and organisations' information security effectiveness
H3a: Leadership is moderate the relationship between knowledge sharing and organisations' information security effectiveness

H4: There is a positive relationship between protection of information and organisations' information security effectiveness
H4a: Leadership is moderate the relationship between protection of information and organisations' information security effectiveness

H5: There is a positive relationship between motivation and organisations' information security effectiveness
H5a: Leadership is moderate the relationship between motivation and organisations' information security effectiveness

H6: Leadership is moderate the relationship between CSF of ISK with organisations' information security effectiveness

Table 5: The List of Constructs and Summaries of Hypotheses

	Independent Variables	Moderator Variable	Dependent Variable
H1	Knowledge	-	Organisations' Information Security Effectiveness
H1a	Knowledge	Leadership	Organisations' Information Security Effectiveness
H2	Employee behaviour	-	Organisations' Information Security Effectiveness
H2a	Employee behaviour	Leadership	Organisations' Information Security Effectiveness
H3	Knowledge sharing	-	Organisations' Information Security Effectiveness
H3a	Knowledge sharing	Leadership	Organisations' Information Security

			Effectiveness
H4	Protection of Information	-	Organisations' Information Security Effectiveness
H4a	Protection of Information	Leadership	Organisations' Information Security Effectiveness
H5	Motivation	-	Organisations' Information Security Effectiveness
H5a	Motivation	Leadership	Organisations' Information Security Effectiveness
H6	-	Leadership	Organisations' Information Security Effectiveness

In summary, knowledge consists of knowledge on password protection, information security behaviour, information security awareness and, training and education. Employee behaviour in this study includes password protection (share password), personal characteristics and attitude towards protection of information security. Knowledge sharing consists of knowledge sharing culture, knowledge sharing behaviour, and relationship. Protection of information includes information security policy, procedures, guidelines, and formal documentation in order to protect information. Last but not least, motivation includes rewards and recognition, incentives, support from colleagues, and organisation support.

Methodology:

This research adapts quantitative research method to address issues under consideration. Questionnaire is used to study the impact of ISK success factors (knowledge, employee behaviour, motivation, knowledge sharing, and protection of information) towards the organisations' information security effectiveness.

In this study, the researcher employ a survey research strategy to answer the research question and fulfil the research purposes. In particular, it seeks to develop a comprehensive research framework and empirically identify the critical success factors of ISK that impact the organisations' information security effectiveness. Malaysian public sector organisation is chose as sampling population and the sample of this research is Information Management and ICT division that includes top management, information security manager, and the end users.

The percentage of number of samples collected from the population in this study is quite high (80.51%). From 590 questionnaires distributed to Malaysians public sector organisations, 481 respondents returned the questionnaires, and out of this, 475 samples are considered completed and usable. Although Sekaran (2006) mentions that in administering questionnaires to the groups or individuals will get a 100% response rate, this study did not achieve the 100% response rate. This is because there are some respondents did not return back the questionnaires. When asked why some of them did not return back the questionnaires, they said that the questionnaire is lost or misplace. There are a few questionnaires that returned with incomplete fill. Researcher assumes that respondents maybe did not understand some of the questions.

Data Analysis:

The collected data are analyse using Statistical Package for Social Sciences (SPSS/version 16) and SmartPLS Version 2.0. The researcher chooses SPSS statistical package is because it facilitates and offers the calculation of all essential statistics such as descriptive statistics and factor analysis. For reliability and validity test, the researcher use SmartPLS Version 2.0.

There are two models in PLS analysis which is measurement model and structural model. It is important to specify relationship in terms of structural and measurement models in order to link operational definitions of constructs of the theory for appropriate empirical test (Hair, Black, Babin, & Anderson, 1998). The measurement model, also known as outer model, depicts the latent variables and their scale items, while the structural model, also known as inner model, specifies the relationship between the exogenous and endogenous variables. In PLS analysis, quality parameters such as internal consistency reliability, convergent validity, discriminant validity, the goodness of fit (GoF) and factor loadings of individual scale items are commonly used to assess the models (Hair *et al*., 1998).

The measurement part of the model is assessed to determine the validity and reliability of the measures used to represent the constructs of interest before examining the structural hypotheses. Validity reveals the extent to which an indicator actually measures what it is supposed to measure while reliability reflects the consistency of measurement (Diamantopoulos & Siguaw, 2000). However, the results and finding of this research are still in progress

Practical Implication and Conclusion:

This study is practical to employee where employee can adapt the ISK in their daily work routines besides treat ISK as a part of job description for them. The second practical implication to the employee is they accept that ISK as a components of information security awareness and training programmes. The third practical

implication of ISK is the proposed framework can be used for security practices among employee. Next, the elements of ISK must be included in information security policy. Lastly, the critical success factors of ISK can be used for measuring information security effectiveness within an organisation.

This on-going research had succeeded in identifying the critical success factors of ISK in organisation which is knowledge, employee behaviour, knowledge sharing, protection of information, and motivation and leadership is the factor that influences all the critical success factors of ISK towards achieving organisational information security effectiveness. The next stage is to test the proposed framework and hypotheses.

REFERENCES

Alavi, M., and D.E. Leidner, 2001. Review: Knowledge management and knowledge management systems: conceptual foundations and research issues. MIS Q., 25(1): 107-136. doi: 10.2307/3250961

Albrechtsen, E., 2007. A qualitative study of users' view on information security. Computers Security, 26(4): 276-289.

Alfawaz, S., K. Nelson and K. Mohannak, 2010. *Information security culture: a behaviour compliance conceptual framework*. Paper presented at the Proceedings of the Eighth Australasian Conference on Information Security - Volume 105, Brisbane, Australia.

Babatunde, D.A., and M.H. Selamat, 2011. Determining factors influencing information security management in the Nigerian Banking and Insurance Sector: a literature review.

Bartol, K.M., and D.C. Martin, 1998. *Management* (3rd ed.). New York: McGraw-Hill.

Belsis, P., S. Kokolakis and E. Kiountouzis, 2005. Information systems security from a knowledge management perspective. Information Management & Computer Security, 13(2/3): 189-189-202.

Birkenkrahe, M., 2002. How large multi-nationals manage their knowledge. Business Review, 4(2): 2-12.

Boonmak, S., 2008. *Influence of Human Factors on Information Security Measures Effectiveness under Ethic Issues*. Paper presented at the 8th Global Conference on Business & Economics, Florence, Italy.

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.

Danish, R.Q., and A. Usman, 2010. Impact of reward and recognition on job satisfaction and motivation: an empirical study from Pakistan. International Journal of Business and Management, 5(2): 159-167.

Davenport, T.H., and L. Prusak, 1998. *Working Knowledge: How Organizations Manage What They Know*. Boston: Harvard Business Review Press.

Diamantopoulos, A., and J.A. Siguaw, 2000. *Introducing LISREL: a Guide for the Uninitiated*. Thousand Oaks, California: SAGE.

Dictionary of Business and Management., 1999. (M. Witzel Ed.). UK: International Thomas Business Press.

Du, R., S. Ai and Y. Ren, 2007. Relationship between knowledge sharing and performance: A survey in Xi'an, China. Expert Systems with Applications, 32(1): 38-46.

Durgin, M., 2007. Understanding the Importance of and Implementing Internal Security Measures. *SANS Institute InfoSec Reading Room*.

Goh, R., 2003. *Information security: the importance of the human element.* (Doctor of Philosophy in Business Administration), Preston University.

Grillo, J.J., 2008. *Examining information security knowledge and vulnerabilities at the Alamo Community College District.* (Northcentral University D.B.A.), Northcentral University, United States -- Arizona. Retrieved from http://search.proquest.com/docview/304823116?accountid=42518 ProQuest Dissertations & Theses (PQDT) database.

Hair, J.F., W.C. Black, B.J. Babin and R.E. Anderson, 1998. *Multivariate Data Analysis*. Upper Saddle River, N.J.: Prentice Hall.

Hennie, K., D. Lynette and S. Tjaart, 2010. A vocabulary test to assess information security awareness. Information Management & Computer Security, 18(5): 316-327.

Herath, T., and H.R. Rao, 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2): 154-165.

Hicks, R.C., R. Dattero and S.D. Galup, 2006. The five-tier knowledge management hierarchy. Journal of Knowledge Management, 10(1): 19-31. doi: 10.1108/13673270610650076

Higgins, E.T., 1998. Promotion and prevention: regulatory focus as a motivational principle. Advance in Experimental Social Psychology, 30: 1-46.

Higgins, E.T., J. Shah and R. Friedman, 1997. Emotional responses to goal attainment: strength of regulatory focus as moderator. Journal of personality and social psychology., 72(3): 515.

Huang, D.L., P.L.P. Rau and G. Salvendy, 2007. A Survey of Factors Influencing People's Perception of Information Security. Lecture notes in computer science, (4553): 906-915.

Jen-Te, Y., 2007. The impact of knowledge sharing on organizational learning and effectiveness. Journal of Knowledge Management, 11(2): 83-90.

Jennex, M.E., and S. Zyngier, 2007. Security as a contributor to knowledge management success. Information Systems Frontiers, 9(5): 493-504.

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: 139-154.

Kuo, T.-S., H. Chi and B. Dorjgotov, 2011. Mediation Effect of Knowledge Management in the Relationship Between Technology and Organizational Effectiveness - an Empirical Study of Mongolian Academy of Sciences. The Journal of Human Resource and Adult Learning, 7(1): 1-10.

Kwo-Shing, H., C. Yen-Ping, R.C. Louis and T. Jih-Hsing, 2006. An empirical study of information security policy on information security elevation in Taiwan. Information Management & Computer Security, 14(2): 104-115.

Leach, J., 2003. Improving user security behaviour. Computers & Security, 22(8): 685-692. doi: 10.1016/s0167-4048(03)00007-5

Lee, J.-N., 2001. The impact of knowledge sharing, organizational capability and partnership quality on IS outsourcing success. Information & Management, 38(5): 323-335. doi: 10.1016/s0378-7206(00)00074-4

Lim, J.S., S. Chang, S. Maynard and A. Ahmad, 2009. *Exploring the relationship between organisational culture and information security culture.* Paper presented at the Australian Information Security Management Conference, Perth, Western Australia.

Malik, M.E., and M.M. Ghafoor, 2011. Organisational effectiveness: a case study of telecommunication and banking sector of pakistan. Far East Journal of Psychology and Business, 2(1): 37-48.

Mittal, Y.K., S. Ro and M. Saxena, 2010a. A Knowledge Management Model to Improve Information Security. IJCSI International Journal of Computer Science Issues, 7(6): 1694-0814.

Mittal, Y.K., S. Roy and M. Saxena, 2010b. Role of Knowledge Management in Enhancing Information Security. International Journal of Computer Science Issues, 7(6): 320-324.

Niekerk, J.F.v., 2005. *Establishing an information security culture in organizations: an outcomes based education approach.* (Degree of Magister Technologiae Dissertation), Nelson Mandela Metropolitan University.

Nikolakopoulos, T., 2009. *Evaluating the Human Factor in Information Security.* (Master thesis), Oslo University College.

Nosworthy, J.D., 2000. Implementing Information Security In The 21st Century — Do You Have the Balancing Factors? Computers & Security, 19(4): 337-347.

Okunoye, A., and N. Bertaux, 2008. Addressing contextual issues in knowledge management: a guiding framework. In M. E. Jennex (Ed.), *Current Issues in Knowledge Management*. USA: Information Science Reference

Oxford Dictionaries, 2012a. Behaviour. Retrieved April,23, 2012, from http://oxforddictionaries.com/definition/behaviour?q=behaviour

Oxford Dictionaries, 2012b. Motivation. Retrieved 3rd May, 2012, from http://oxforddictionaries.com/definition/motivation?q=motivation

Parsons, K., A. McCormac, M. Butavicius and L. Ferguson, 2010. Human factors and information security individual, culture and security environment. Edinburgh, South Australia: Command, Control, Communications and Intelligence Division, Defence Science and Technology Organisation.

Ping, A.W., 2010. *Information security knowledge and behavior: An adapted model of technology acceptance.* Paper presented at the Education Technology and Computer (ICETC), 2010 2nd International Conference

Risvold, M.O., 2010. *Organisational issues related to information security behavior.* (Master Thesis, Continuation Courses), Lulea University of Technology.

Sallis, E., and G. Jones, 2002. *Knowledge Management in Education*. London, UK: Kogan Page Limited.

Sandhu, M.S., K.K. Jain and U.K. Ahmad, 2011. Knowledge sharing among public sector employees: evidence from Malaysia. International Journal of Public Sector Management, 24(3): 206-226.

Sekaran, U., 2006. *Research Methods for Business : A Skill-Building Approach*. UK: John Wiley & Sons Inc.

Shuangyan, L., C. Chinghang and K. Lamfor, 2006. *A knowledge framework for information security modeling.* Paper presented at the Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia.

Siu, M.L., and W. Hui, 2011. *The effects of knowledge on security technology adoption: Results from a quasi-experiment.* Paper presented at the Information Science and Service Science (NISS), 2011 5th International Conference on New Trends in.

Thomson, K.-L., and R. Von Solms, (2006). Towards an information security competence maturity model. Computer Fraud & Security, (5): 11-15.

Thomson, K.-L., R. Von Solms and L. Louw, 2006. Cultivating an organizational information security culture. Computer Fraud & Security, (10): 7-11. doi: 10.1016/s1361-3723(06)70430-4

Whitman, M.E., and H.J. Mattord, 2012. Principles of Information Security (4 ed.). U.S.A: Course Technology.

Wirtz, J., and M.O. Lwin, 2009. Regulatory focus theory, trust, and privacy concern. Journal of Service Research, 12(2): 190-207.

Zakaria, O., 2006. Internalisation of Information Security Culture amongst Employee through Basic Security Knowledge. In S. Fischer-Hubner, K. Rannenberg, L. Yngstrom & Lindskog (Eds.), *IFIP International Federation for Information Processing* (Vol. 201): Springer Link.

Zakaria, O., 2007. *Investigating information security culture challenges in a public sector organization: a Malaysian case*. Royal Holloway, University of London.