Journal of Theoretical and Applied Information Technology
10th November 2013. Vol. 57 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE RELATIONSHIP OF INFORMATION SECURITY KNOWLEDGE (ISK) AND HUMAN FACTORS: CHALLENGES AND SOLUTION

[1]ROHANA MOHAMAD RASHID, [2]OMAR ZAKARIA, [3]MOHD NABIL ZULHEMAY

[1]Faculty of Defence Science and Technology, National Defence University of Malaysia, Malaysia

[2]Assoc. Prof., Faculty of Defence Science and Technology, National Defence University of Malaysia, Malaysia

[3] Faculty of Defence Science and Technology, National Defence University of Malaysia

E-mail: [1]rohana.mrashid@gmail.com , [2]omar@upnm.edu.my, [3]nabilzulhemay@gmail.com

ABSTRACT

Information, knowledge, and information security are indispensable in an organisation to ensure the effectiveness of an organisation. An organisation needs people who have adequate information and knowledge to run a business. Lack of knowledge especially in information security may jeopardise the organisation such as the increase of internal security incidents. Human factors will also influence the effectiveness of an organisation. Therefore, adopting the right behaviour in daily work routines may increase the effectiveness of the organisation. There is a need to educate everybody in the organisation regarding information security and security awareness, training, and education programme in cultivating good behaviours in the organisation. The relationship between human factors, information security, knowledge, and knowledge management can be encompassed by the term 'information security knowledge'. This paper has developed a clear definition of information security knowledge so that it can be used to guide employees in implementing information security practices within the organisation. Applying information security knowledge in the organisation may help decrease the internal security incidents that are posed by humans hence will lead to the organisational information security effectiveness.

Keywords: *Human Factor; Knowledge; Information Security; Information Security Effectiveness; Information Security Knowledge; Knowledge Management*

1. INTRODUCTION

In today's life, information, knowledge, and information security play an important role especially in an organisation. People use information to make decisions. People use knowledge to create new knowledge and people use information security to protect information assets. Lack of information, knowledge, and information security will jeopardise the organisation and give a negative impact to organisational effectiveness. We know that the origin of information is from data, and information will produce knowledge. There are many authors, researchers, and scholars who had defined data, information and knowledge, and the relationship between them. In this paper, only the most cited definitions are included.

Data are raw materials which carry information such as numbers, words, diagrams, images, sound, smell, touch, and taste [1]. Raw data are useless (do not have any meaning) until they are organised or manipulated in such a way that they provide information [2]. Davenport and Prusak [3] describe information as a message that is usually in the form of documents or an audible and visible communication. This statement is supported by the It Governance Institute [2] and Liew [1], who describe information is a message that has relevant meaning, implication, or input for decision or action. Information has purposes. Basically, the purpose of information is to aid in making decisions or solving problems [1]. Information is the foundation of knowledge. Davenport and Prusak [3] opine knowledge as a fluid mix of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experience and information. In addition, Alavi and Leidner [4] posit knowledge as a justified personal belief that increases an individual's capacity to take effective action. Knowledge originates and is applied in mind. Kelley [5] adds knowledge happens only when a human experiences and his insights are applied to data and information. Table 1 depicts the relationship between data, information, and knowledge hierarchy with factors of interest in an information security's example.

Table 1: Data, Information And Knowledge With Factors Of Interest In Information Security's Example

Data, information, knowledge hierarchy	Factors of interest in information security (Examples)
Data	Facts (numbers, words, images, etc.)
Information	Policies, procedures, books, reports, posters, etc. (Information security awareness programme)
Knowledge	Skills and experience (Information security training programme)

In an organisational context, knowledge is often embedded not only in the documents or repositories but also in the organisational process, practices, routines and norms [6]. In the organisation, information and knowledge become recognised as information assets and also organisational assets [2, 7]. Therefore it is important to protect these organisational assets from being exposed because nowadays, internal security incidents have increasingly become a serious problem in the organisation. As a result, information security needs to be implemented and managed within the organisation to ensure the information is secure. In order to improve the organisation's performance and effectiveness, knowledge management should be practised because it involves the ideas and experience of employees, customers and suppliers [8]. Furthermore, knowledge management encourages knowledge to be created, shared, learnt, enhanced, and organised, for the benefits of the organisation [9]. Therefore, the integration of information security and knowledge management is important in the organisation where all elements on information security and knowledge management are consolidated in order to protect the organisation's asset and at the same time increase organisational performance. This is where the term of information security knowledge is introduced. The term information security knowledge will be defined later.

When discussing internal security incidents, of course they involve attacks on the people inside the organisation such as the employee, contractor, or third party support technician who can run the software and or make a change that has negative impacts to the organisation [10]. From the three resources of internal security incidents, this paper will focus on the employees in organisations who are responsible in running the business process in their daily work routines and also can be categorised as human factor issues which is also emphasised in this paper.

Therefore, the purpose of this paper is to investigate the relationship between human factors, information security, knowledge and knowledge management. It also plans to develop a clear definition of information security knowledge that can be used to guide employees in implementing information security practices within organisations.

2. INFORMATION SECURITY

Security and information security are two different things. Security is the process of reducing risk or threats that can jeopardise an organisation meanwhile information security is a business requirement to protect the organisation's investment in its information assets [7]. Many researchers and scholars have discussed the definition of information security. 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 [11]. The Committee on National Security System (CNSS) defines information security as the protection of information and its critical elements. The elements include the systems and hardware that are used to store and transmit the information [12]. C.I.A. triangle, the paramount model in information security, also called the information security triad, is always highlighted when the issues of information security are discussed.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Overall the most important thing about information security is protecting information assets from being disclosed, integrity violation, and denial of service. However, people need knowledge in information security to ensure the effectiveness of information security in the organisation which in turn can help minimise the internal security incidents.

3. KNOWLEDGE AND KNOWLEDGE MANAGEMENT

Although knowledge is derived from information, knowledge also can become information. This is explained by Alavi and Leidner [13] 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 [14].

There are two types of knowledge which are tacit knowledge and explicit knowledge. The idea of tacit knowledge was first identified by Polanyi (1969), who is widely accepted as the founding father in tacit knowledge. Polanyi's aim was to bring up the inarticulate dimension of human knowing. In his paper, he saw tacit knowledge is not just a category of knowledge, but tacit knowledge is a process. This concept actually had been introduced by Gilbert Ryle a few years earlier as "knowing how" which referred to a practical way of knowing how to do things [15].

Nonaka and Takeuchi [16] popularise tacit knowledge in the management literature. Tacit knowledge is something not easily visible and expressible. It is highly personal and hard to formalise, and it is difficult to be communicated or shared with others. Subjective insights, intuitions, and hunches are the examples of tacit knowledge. Furthermore, tacit knowledge is deeply rooted in an individual's action and experience, as well as in the ideals, values, or emotions [16]. Kikoski and Kikoski [17] view tacit knowledge as personal knowledge and is hard to formalise. It is rooted in action, procedures, commitment, values, and emotion. Tacit knowledge is not codified, it is not communication "language", and it is acquired by sharing experiences, by observation and imitation [17, 18].

On the other hand, explicit knowledge is more formal and systematic. Explicit knowledge can be expressed in words and numbers and easily communicated and shared in the form of hard data, scientific formula, codified procedures, or universal principles [16]. Kikoski and Kikoski [17] describe explicit knowledge as what can be embodied in a code or a language and as a consequence it can be verbalized and communicated, processed, transmitted, and stored relatively easily. Books, journals, and mass media such as newspapers, television, internet, and many more are the examples of explicit knowledge [19].

Once this paper investigate the usage of information and knowledge within organisation, knowledge management is appropriate to be adapted. Knowledge management includes the process of identifying and mapping intellectual assets within the organisation, create new knowledge for competitive advantage within the organisation, making vast amounts of corporate information accessible, practise knowledge sharing, and technology that enables all of the above that include groupware and intranets [20]. This statement is supported by Davenport, et al. [21] who view knowledge management as a development of knowledge assets in the organisation and includes both tacit (subjective) and explicit (documented) knowledge. Knowledge management involves the identification, sharing, and creation of knowledge process.

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 [22]. 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" [23].

Ikujiro Nonaka and Hirotaka Takeuchi are two names that are very synonym with knowledge management. They propose a model of knowledge creating process to understand the nature of knowledge creation. The model is known as SECI model or also called as 'modes of knowledge creation'. The model includes four processes of knowledge creation which are **S**ocialisation, **E**xternalisation, **C**ombination, and **I**nternalisation.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2 shows the description of each process in the SECI model with the factors of interest in information security example.

Table 2: Knowledge Creation Modes In Information Security Example

Modes	***Description***	***Factors of interest in information security (Example)***
Socialisation	-Sharing tacit knowledge through face-to-face communication or shared experience	Information security awareness, training and education
Externalisation	-A process where individuals take existing knowledge and their tacit knowledge and create something new that organisation can share.	Documentation, manuals, policies, procedures
Combination	-Combination of various elements of explicit knowledge. -Integrate, modify, combine, upgrade, and remodel the existence explicit knowledge into new explicit knowledge.	Blueprint of information security awareness programme
Internalisation	-By referring to explicit knowledge, with addition of own interpretation, review, research, and other knowledge process method, a new tacit knowledge is created.	Seminar, brainstorming, workshop, colloquium on information security

All the knowledge creation modes are applicable in information security as shown in Table 2. This implies that the integration of information security and knowledge management is very significant especially in achieving organisational effectiveness.

4. CHALLENGES IN INFORMATION SECURITY AND KNOWLEDGE MANAGEMENT WITHIN HUMAN FACTOR

There are many challenges faced by information security knowledge in terms of human factor. The issues in human factor in information security have been much debated [24-28]. Human or people is one of the principle factors in knowledge management and information security. Abell and Oxbrow [9] view people as an important ingredient to the construction of information security, and the effectiveness of information security in an organisation will require strong commitment from the various levels in the organisation. Here, everybody in the organisation is responsible in managing and protecting the information assets which are the integrity, confidentiality, and availability to achieve information security effectiveness. As It Governance Institute [2] 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 biggest challenges in information security and knowledge management are from human/ people in the organisation. People in the organisation have the potential to cause more damage to the organisation and they also have many advantages to attack the organisation without being detected by others [29]. With the legitimate and access to facilities and information, knowledge of the organisation and its process and knowing the exact location of the valuable information, they will

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

easily intrude without leaving any trace. Consequently people, as a part of a system and organisation are always going to be the weak point in information security in organisation. Human and knowledge are very interrelated because the organisation cannot create new knowledge without them. As said before, knowledge originates and is applied in minds and only humans have minds that are needed in making decisions for competitive advantages.

The second challenge in information security and knowledge management is from information technology. With the development of information technology, there are many threats evolving around information security. In accordance to that notion, a lot of security software are designed to protect information from being hacked and misused either by internal or external sources that may cause the security incidents in organisations such as firewalls, intrusion detection systems, antivirus solutions, and many more. Each of the security software is designed with specific function apart from protecting the system. Nevertheless, the security incidents are still occurring even when the best security software with the advance technology and the most secure algorithms are used. This is because there will always be human's involvement in every process and implementation of the system and the weakness of human is human makes mistakes. Pipkin [7] clarifies by giving an example of human's mistake. By dragging and dropping information into the wrong spot can be catastrophic. What appears to be a simple action may create a great amount of work to repair.

Lack of knowledge sharing in organisation is also one of the challenges in information security and knowledge management in organisation. In knowledge management environment in the public sector in Malaysia, 83% of public sector personnel believed that their knowledge belongs to their agency alone and they are reluctant to share it with other entities [30]. As a result they did not practise knowledge sharing culture within organisations [30]. This is because they presume their organisation's knowledge as their own intellectual property.

There are some knowledge and information that can be shared. For instance, knowledge on how to protect document using password protection must be shared. They are many benefits of knowledge sharing culture such as people can learn from shared experience through best practices; as an entry point for connecting people, people to document, and vice versa; and first-hand knowledge transfer from employer to employee.

In accordance with that, an organisation should use an enlightened approach to share knowledge and information. Information security takes a larger view that an organisation's information and knowledge must be protected irrespective of the way the information is handled, processed, and transported or stored. Therefore, there is a need to emphasise on the non-technical measures such as education, training, and awareness and also fostering information security culture among employee in organisation [29, 31, 32].

5. INFORMATION SECURITY AWARENESS, TRAINING, AND EDUCATION PROGRAMME: A SOLUTION TO HUMAN'S PROBLEM

It is obvious that everybody in the organisation need to be educated about the importance of security awareness and also incorporated behavioural training [27]. Moreover, Albrechtsen [32] adds having information security awareness may raise individual's security awareness and it is a good starting point for building a corporate security culture based on common values and attitude. Every people in the organisation must have the awareness on information security and must react positively in line with the awareness. According to Al-Awadi and Renaud [33], awareness and training programme is one of the success factors in information security implementation in organisations where it would give a significant impact in helping organisations to achieve organisation's information security effectiveness. Hagen and Albrechtsen [34] point out that information security awareness has a significant effect in improving user's security knowledge and behaviour. Once people are aware of information security, they will know which behaviour should be applied and practiced in order to minimise the number of internal security incidents in an organisation. Furthermore, according to Colwill [29], having information security awareness may change people's behaviour and also enhance the level of trust between an employer and his employees.

The next step is conducting information security training programme that is monitored by top management. Employees will be able to obtain more knowledge as needed which are knowledge in design, implementation, or security programme operation for organisation and system. In addition,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the skills and knowledge on computers and system can be developed while the level of security awareness is being improved [35]. According to Whitman and Mattord [35], information security training programmes should address the following issue: (1) the information security educational components required of all information security professionals, and (2) the general educational requirements that all information technology professional must have. Whitman and Mattord [35] also stress on training at knowledge level where skills are important in order to solve problems. Moreover, adding the knowledge management element/processes such as knowledge creation and knowledge sharing towards the protection of information is very beneficial to the organisation.

Training is most effective when it is designed for a specific category of users [35]. As proposed by Niekerk [25], 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. In accordance with that, Colwill [29] believes that providing education on the importance of protecting organisation's information is one of the initial steps in creating awareness among employees. This is because, when everybody is educated, their knowledge will increase. With knowledge provided by the organisation, they will learn the new knowledge, share with others and practise and use it in their daily work routine. In order to protect the information assets, everybody in the organisation should have knowledge on information security parallel with knowledge on their roles and responsibilities.

All users whether IT personnel or top management, are the end users. Based on the definition in MyMIS MAMPU, a user is anyone who accesses any ICT asset. A user maybe an employee, members of the administration, contractors, vendors, or anyone who accesses or uses ICT assets [36]. Meanwhile IT personnel include security manager, security administrators/ analyst, security staffer, and also security officer/ investigator. In information security department, the top management is known as CISO or CSO. All users have different knowledge based on their roles and responsibilities regarding their work. Table 3 shows the categories of users with the minimal knowledge needed.

Table 3: Categories Of Users With The Minimal Knowledge Needed By Thomson [37]

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 emails.
IT Personnel	-Knowledge and education on information security technical controls.
Top Management	-Knowledge and education on users' training. -Knowledge and education on information security policy, procedures, and controls in organisation. -Knowledge in decision making.

Although an IT user in an organisation has his own knowledge on his roles and responsibilities in his job routines, he must have the minimal knowledge as stated in Table 3 in the 'End User' column. It is important to have this minimal knowledge other than his specific roles and responsibilities. In addition a user must understand, support, acknowledge, and abide the organisation's ICT security policy, standards and guidelines [36].

Pipkin [7] adds, when people know how to use the system that they are expected to use, they are more productive and less likely to make mistakes. Furthermore, when people understand the importance of information security, how to use it, and where to report if incidents occur, they can help reduce the internal security incidents within an organisation and at the same time can increase the organisational effectiveness. This is true and supported by Whitman and Mattord [35] where they conclude that security awareness, training, and education programme can improve employees' behaviour in handling information properly, and at the same time make employees accountable for their actions.

6. INFORMATION SECURITY KNOWLEDGE (ISK) : A RELATIONSHIP WITH HUMAN FACTOR

Both information security and knowledge management need human factor to start the process. There is nothing can be done without the intervention of human factor. Furthermore, employee which is the human factor in organisation is the most important assets other than information.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Every employee need to know the importance of information security in order to protect their organisation assets. Therefore, understanding and applying information security knowledge is vital. This implies that, human must have appropriate behaviour and attitude towards information security. Knowledge and behaviour should be in line so that the effectiveness of information security in organisation will be achieved. This indicates that there is relationship between human, information security, knowledge and also knowledge management and Figure 1 depicts the relationship. It is pointless if human has knowledge but did not pose the appropriate attitude towards information security. This problem will lead to the ineffectiveness of information security and will contribute to the internal security incidents in organisation. Therefore, there is a need to emphasise on the importance of having the correct attitude towards information security in security education, and training programme.

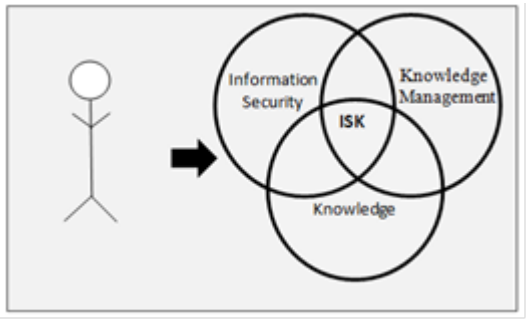

Figure 1: Relationship Between Human Factor and ISK

The relationship of information security, knowledge, and knowledge management is encompassed by the term 'information security knowledge'. Defining 'Information Security Knowledge' includes combining all related elements in information security, knowledge and knowledge management. Table 4 indicates the element of information security knowledge that are extracted from the elements in information security, knowledge management, and knowledge.

Table 4: 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

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

7. CONCLUSION

Human factor plays an important role in an organisation. Humans themselves are the ones who can put the organisational effectiveness in a dangerous situation and also the ones who can protect the organisational effectiveness. Besides, top management must be made aware that the protection of information security is the responsibilities of all users. Therefore, by providing information security knowledge that includes information security awareness, training, and education programme may save the organisation from adverse events.

This paper defines the term 'Information Security Knowledge'. It explored the relationship between the four fields of human factor, information security, knowledge, and knowledge management and highlighted the importance of binding these fields together. Having a clear definition of information security knowledge will help researchers to proclamation the term especially in information security context. Furthermore, it is important to have a clear definition of information security knowledge so that it will help employees as guidance in implementing information security practices within organisation. However, this

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

definition is limit to the information security context. Other field may have the other definition.

Further research will be conducted to investigate the impact of information security knowledge on human factor towards the organisational information security effectiveness and identify the critical human factors of information security knowledge of the Malaysian public sector.

ACKNOWLEDGEMENT

This paper is fully funded by Centre of Research and Innovation, National Defence University of Malaysia, Malaysia.

REFERENCES

[1] A. Liew, Understanding Data, Information, Knowledge And Their Inter-Relationships, *Journal of Knowledge Management Practice*, vol. 8, 2007.

[2] IT Governance Institute. (2006). *Information Security Governance Guidance For Boards Of Directors And Executive Management*. Available: http://www.books24x7.com/marc.asp?bookid=30815

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

[4] M. Alavi and D. E. Leidner, Knowledge management systems: Issues, challenges, and benefits, *Communications of AIS*, vol. 1, pp. 1-38, 1999.

[5] J. Kelley, *Knowledge Nirvana: Achieving the Competitive Advantage through Enterprise Content Management and Optimizing Team Collaboration*. USA: Xulon Press, 2002.

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

[7] D. L. Pipkin, *Information Security: Protecting the Global Enterprise*. Upper Saddle River, New Jersey: Prentice Hall, 2000.

[8] M. Skapinker and Chartered Institute of Personnel and Development, Knowledge management : the change agenda, ed: CIPD, 2002.

[9] A. Abell and N. Oxbrow, *Competing With Knowledge : The Information Professional in the Knowledge Management Age*. London: Facet Publishing: TFPL, 2001.

[10] M. Durgin. (2007) Understanding the Importance of and Implementing Internal Security Measures. *SANS Institute InfoSec Reading Room*. Available: http://www.sans.org/reading_room/whitepapers/policyissues/understanding-importance-implementing-internal-security-measures_1901

[11] Cyber Security Malaysia, MS ISO/IEC 27001:2007 Information Security Management System (ISMS) Implementation, ed. Malaysia: Cyber Security Malaysia, 2010.

[12] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 4th ed. Australia: Course Technology, 2012.

[13] M. Alavi and D. E. Leidner, Review: Knowledge management and knowledge management systems: conceptual foundations and research issues, *MIS Q.*, vol. 25, pp. 107-136, 2001.

[14] R. C. Hicks, R. Dattero, and S. D. Galup, The five-tier knowledge management hierarchy, *Journal of Knowledge Management*, vol. 10, pp. 19-31, 2006.

[15] F. Oguz and A. E. Sengun, Mystery of the unknown: revisiting tacit knowledge in the organizational literature, *Journal of Knowledge Management*, vol. 15, pp. 445-461, 2011.

[16] I. Nonaka and H. Takeuchi, *The Knowledge Creating Company: How Japanese Companies Create the Dynamics of Innovation*. New York: Oxford University Press, 1995.

[17] C. Kikoski and J. Kikoski, *The Inquiring Organization: Tacit Knowledge, Conversation, and Knowledge Creation: Skills for 21st-Century Organizations*. London: Praeger, 2004.

[18] R. Hall and P. Andriani, Managing knowledge for innovation, *Long Range Planning*, vol. 35, pp. 29-48, 2002.

[19] R. S.-d. Alwis and E. Hartmann, The use of tacit knowledge within innovative companies: knowledge management in innovative enterprises, *Journal of Knowledge Management*, vol. 12, pp. 133-147, 2008.

[20] R. O. Barclay. (1997, 6rd March). *Knowledge Praxis*. Available: http://www.imamu.edu.sa/Scientific_selections/abstracts/Abstract%20%20IT%20%203/What%20Is%20Knowledge%20Management.pdf

[21] T. H. Davenport, D. W. D. Long, and M. C. Beers, Successful knowledge management

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

projects, *Sloan Management Review*, vol. 39, pp. 43-57, 1998.
[22] E. Sallis and G. Jones, *Knowledge Management in Education*. London, UK: Kogan Page Limited, 2002.
[23] M. Birkenkrahe, How large multi-nationals manage their knowledge, *Business Review*, vol. 4, pp. 2-12, 2002.
[24] S. Boonmak, Influence of Human Factors on Information Security Measures Effectiveness under Ethic Issues, presented at the 8th Global Conference on Business & Economics, Florence, Italy, 2008.
[25] J. F. v. Niekerk, Establishing an information security culture in organizations: an outcomes based education approach, Degree of Magister Technologiae Dissertation, Faculty of Engineering, Nelson Mandela Metropolitan University, 2005.
[26] T. Nikolakopoulos, Evaluating the Human Factor in Information Security, Master thesis, Network and System Administration, Oslo University College, 2009.
[27] K. Parsons, A. McCormac, M. Butavicius, and L. Ferguson, Human factors and information security individual, culture and security environment, ed. Edinburgh, South Australia: Command, Control, Communications and Intelligence Division, Defence Science and Technology Organisation, 2010.
[28] M. O. Risvold, Organisational issues related to information security behavior, Master Thesis, Continuation Courses, Computer and System Science, Department of Business Administration and Social Sciences, Lulea University of Technology, 2010.
[29] C. Colwill, Human factors in information security: The insider threat – Who can you trust these days?, *Information Security Technical Report*, vol. 14, pp. 186-196, 2009.
[30] Malaysia Administrative Modernisation and Management Planning Unit (MAMPU), Knowledge Management Blueprint, ed, 2011.
[31] Y. K. Mittal, S. Roy, and M. Saxena, Role of Knowledge Management in Enhancing Information Security, *International Journal of Computer Science Issues*, vol. 7, pp. 320-324, 2010.
[32] E. Albrechtsen, A qualitative study of users' view on information security, *Computers Security*, vol. 26, pp. 276-289, 2007.
[33] M. Al-Awadi and K. Renaud, Success factors in information security implementation in organisations, in *IADIS International Conference e-Society 2007*, Lisbon, Portugal, 2007, pp. 169-176.
[34] J. M. Hagen and E. Albrechtsen, Effects on employees' information security abilities by e-learning, *Information Management & Computer Security*, vol. 17, pp. 388-407, 2009.
[35] M. E. Whitman and H. J. Mattord, *Management of Information Security*, 3rd ed. United States of America: Course Technology, 2010.
[36] Malaysia Administrative Modernisation and Management Planning Unit (MAMPU), Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS), P. M. s. Department, Ed., ed. Malaysia: Perpustakaan Negara Malaysia, 2001.
[37] M. Thomson, The development of an effective information security awareness program for use in an organization, ed. Port Elizabeth, South Africa: Port Elizabeth Technikon, 1998.