International Business Management 10 (17): 3982-3991, 2016
ISSN: 1993-5250

Generic Taxonomy of Assets Identification During Risk Assessment in Information Security Management

[1]Palaniappan Shamala and [2]Rabiah Ahmad
[1] Faculty of Computer Science and Information Technology,
University Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia
[2]Center for Advanced Computing Technology,
Faculty of Information and Communication Technology,
University Technical Malaysia Melaka (UTEM), Melaka, Malaysia

Abstract: Information Security Risk Assessment (ISRA) is a vital method for organizations to develop effective and economically-viable control strategies. Organizations wanting to eliminate the possible risks in their organizations by identifying and prioritizing information assets. However, current ISRA methods have critical limitations whereas they adopt mainly on the technicality of organizational assets while, discounting people as knowledgeable entities of the organization and neglecting unofficial copies of assets which are created in any given work environment. A structured approach by Webster and Watson used as guidelines for determining the source material for the review. The result shows the limitation have been discussed separately by various researchers but none of the researchers have combines all the human related non-technical perspective assets together under one frame. This study presents a taxonomy of assets for ISRA with an integration and comprehensive overview of technical and non-technical perspective assets. This taxonomy able to guide ISRA practitioners to examine which assets are most important and enables them to collect all the needed information associated with assets in the early process of their actual ISRA implementation.

Key words: Traditional ISRA, asset identification, taxonomy, technical assets, non-technical assets, information leakage

INTRODUCTION

Information on new developments and innovations in the business world is an enormously valuable resource to any organization for decision-making and for the continuance of high-standard business operations (Gerber and von Solms, 2005). The rapid growth of today's broadband networks and high-capacity electronic data storage technologies enable the organizations and individuals to use electronic forms of information in their daily activities. Organizations are becoming increasingly aware that the security of their information is of paramount importance. This is because lax security incidents can lead to severely adverse consequences for organizations, such as substantial losses to industry through the direct loss of information assets and financial impact, a loss in organizational reputation and customer confidence and a loss of employee productivity or even risks pertaining to legal issues (Alberts and Dorofee, 2002; Shedden *et al*., 2010, 2011).

Undoubtedly, information security plays a great and important role in organizations not to only maintain confidentiality and integrity but also availability, non-repudiation, accountability, authenticity and reliability. Therefore, organizations achieve an ideal level of information security by applying Information Security Risk Assessments (ISRA) to conduct risk analysis to identify and evaluate risks and then employing risk management techniques to mitigate or reduce risk where deemed appropriate (Baskerville, 1991; Dhillon and Backhouse, 2001; Shedden *et al*., 2011, 2010).

Generally majority of ISRA methods only concentrate on tangible assets where the focus is on technical perspective assets alone (Alnatheer and Nelson, 2009; Bandyopadhyay *et al*., 1999; Rainer *et al*., 1991; Onwubiko and Lenaghan, 2007; Shedden *et al*., 2009, 2010, 2011; Spears, 2006; Stolen *et al*., 2002). ISRA mainly focusses on analyzing vulnerabilities and threats to the information resources and deciding what counter measures to take for reducing risk to an acceptable level

Corresponding Author: Palaniappan Shamala, Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia

(Feng *et al*., 2014). Organizations have to revise the process of ISRA risk management methods by incorporating non-technical perspective assets into the identification of information security assets (Shedden *et al*., 2009, 2010, 2011; Spears, 2006).

To address these issues, this study employs a newly developed taxonomy of technical and non-technical perspective assets in ISRA's asset identification. The taxonomy is divided into two categories namely technical and non-technical perspectives. The technical perspective assets are identified by carrying out a comparative study between the existing risk management methodologies which are known as traditional ISRA methods. While the non-technical assets were figured out based on the shortcomings in existing ISRA methods which have critical limitations in adopt a technical perspective. Reviews and analysis were done to identify a comprehensive set of non-technical assets by focusing on previous research issues to address these shortcomings.

This study identifies and discusses the importance of people and their knowledge as assets of the organizations; and incomplete views of organizations towards day-to-day activities where employees creating and using unofficial assets are also considered as confidential assets. Based on the results of the analysis, this study suggests a taxonomy of technical and non-technical perspective information security assets in order to give a broader view guided with a proper list of assets to be protected. Practitioners would be able not only to understand all the possible assets in the organization but also be able to collect all the needed information associated with assets before and during their actual ISRA implementation.

Related work: ISRA is a vital element for small and multi-national organization in protecting their information assets. ISRA is introduced among organizations to identify and prioritize information assets such as, the specific threats that an organization induce; the chance of these threats occurring and the impacts on the business. The necessity for ISRA in an organization has increased mainly because the changes in structure and the nature of information technologies applied to information can potentially create risks. Although, there is a wide range of definition for risk, within the computer environment the definition of risk in the context of this study is "the potential for damage to a system or associated assets that exists as the result of the combination of a security threat and a vulnerability" (Kailay and Jarratt, 1995).

According to Shedden *et al*. (2010, 2009), state that typical ISRA is composed of three phases context establishment, risk identification and risk analysis. Among these three phases, 'risk identification' will be the most important phase for organizations to discover and select an organization's most critical information assets. Risk identification consists of three sub steps namely, asset identification, threat identification and vulnerability identification.

Limitation of traditional risk analysis: Traditional risk analysis methods are widely accepted because they are more focused on technology. Since, these methods comply with industry accepted security guidelines, an extensive list of known threats and vulnerabilities towards technical assets are publicly available. Thus, organizations can conduct technology based risk analysis with out any reservations. According to Salmela (2008), the traditional risk analysis methods are well established for investigating the existence of technology based risks as there are similarities in every phenomen on that occurs. According to Halliday *et al*. (1996), traditional risk reviews are usually not carried through to a Business Impact Analysis (BIA). BIA is required in the development of a business continuity plan. Spears' (2006) studies have listed three limitation in traditional risk analysis. However, this study focuses on people and processes as they are given the least importance as significant sources of security risk.

Nevertheless, today technology has advanced rapidly where networked computers are almost ubiquitous. Despite employing technology based security such as firewall, virus protection software, intrusion detection systems and other advanced technologies, the organization's computers, networks and information are still facing high security risks (Jourdan *et al*., 2010; Kolokotronis *et al*., 2002; Richardson, 2008).

Therefore, several researchers (Halliday *et al*., 1996; Kolokotronis *et al*., 2002; Salmela, 2008; Shedden *et al*., 2010, 2011; Spears, 2006; Suh and Han, 2003) have argued over the need for organizations to employ business analysis methods to provide a more comprehensive view on potential business losses.

MATERIALS AND METHODS

Research approach: This study is developed based on the research approach presented in Fig. 1 in order to identify the non-technical perspective assets which are not handled by current ISRA methods. In the first stage, a comparative analysis conducted to find mutual list of important assets to be protected. These comparative analysis are done between six types of ISRA methodologies known as Professional Organization namely: CRAMM (Bornman and Labuschagne, 2004; Sarkheyli and Ithnin, 2010; Siemens, 2005; Yazar, 2002), CORAS (Aagedal *et al*., 2002; Bornman and Labuschagne, 2004; De Braber *et al*., 2007; Dahl, 2008; Fredriksen *et al*.,

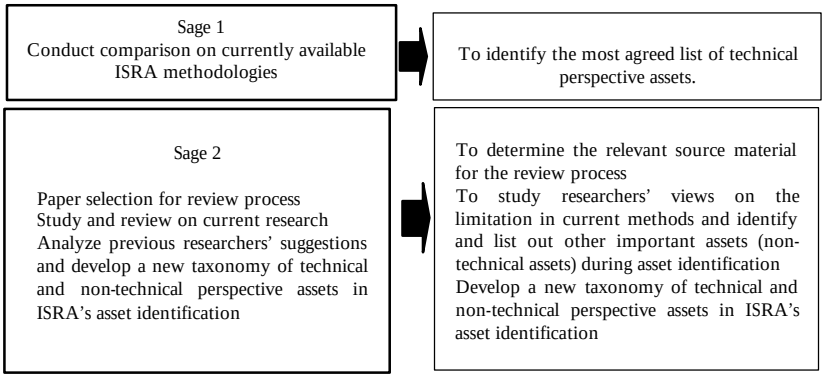

Fig. 1: Research approach for identifying the non-technical perspective assets in ISRA

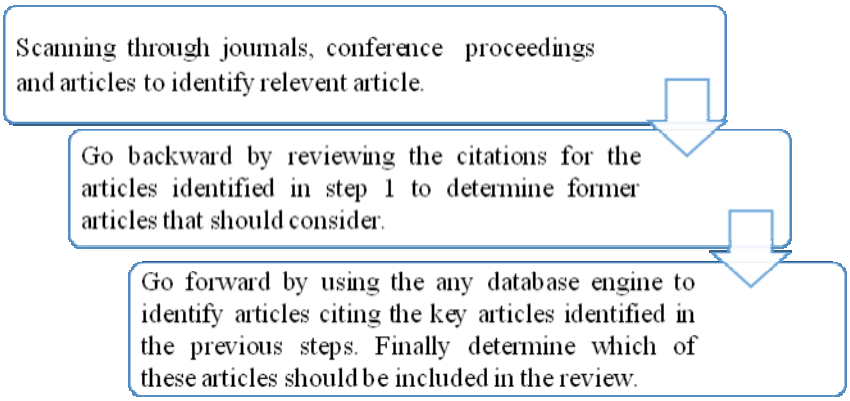

Fig. 2: Step to identify relevant materials for review (Webster and Watson, 2002)

2002; Lund *et al*., 2011; Raymond, 1995; Refsdal, 2011a, 2011b; Vorster and Labuschagne, 2005), OCTAVE (Albert and Dorofee, 2001; C. Alberts *et al*., 2003, 2001; Bornman and Labuschagne, 2004; Elky, 2006; Sarkheyli and Ithnin, 2010; Visintine, 2003; Vorster and Labuschagne, 2005): Research Project: ISRAM (Karabacak and Sogukpinar, 2005; Vorster and Labuschagne, 2005), Risk Analysis Is Based On Business Models (Suh and Han, 2003; Vorster and Labuschagne, 2005) and International Organization: NIST 800-30 (NIST, 2010, 2011a, 2012; Stoneburner *et al*., 2002; Syalim *et al*., 2009). The list of agreed assets among the six ISRA methodologies were chosen based on the highest frequency of 'most often agreed' responses.

In the next stage, papers related to current views of assets which adopt a limited view of information assets during asset identification are identified. The materials selected for this review were the result of conforming to recommendations proposed by Webster and Watson (2002) to conduct a structured approach to determine the source material for the review. According to Webster and Watson (2002), there are three steps to identify relevant materials as in Fig. 2. Based on the structured approach explained in Fig. 2, the process of paper selection for review was accomplished. The identification of relevant studies was based on an examination and study of papers found through manual inspection of papers by querying the Scopus database. The search included all the articles in the journal and conference proceedings. Any study with the title, abstract or keywords that contain "information security risk", "asset identification", "business perspective" and "information" was identified. These key phase were used as a term in this search to find articles from 2004 to present. In total, 68 papers were found. Once again the search was limited as below:

- Subject: computer science and engineering
- Source type: conference proceedings and journals
- Language: english

After vetting based on the limitation, a total 47 papers were short-listed. All the papers were examined by using manual inspection of title and if unsure, the abstracts. Only 6 articles relevant to the review were selected. By referring to the citations listed in the articles

identified in step 1, additional articles which were deemed relevant to the topics was determined. Finally, Google Scholar was used to find articles citing the key articles in the previous step. Another technique that was used to find relevant articles was by using "Cited by" tool in Google Scholar. This technique further enhanced the opportunity of finding related articles in the same areas of concern. This yielded 14 additional articles relevant to the review topics. Overall, 20 articles (Ahmad *et al*., 2005; Belsis *et al*., 2005; Bernard, 2007; Botha and Eloff, 2001; Choo, 2000; CISCO, 2008a, b; Fenz and Ekelhart, 2009; Halliday *et al*., 1996; Kolokotronis *et al*., 2002; Liu *et al*., 2006; Ramli and Aziz, 2012; Salmela, 2007; Sanchez, 2004; Shedden *et al*., 2009, 2010, 2011; Spears, 2006; Suh and Han, 2003; Zakaria, 2006) were collected to review and were duly analyzed to design the taxonomy of assets for information security risk assessment.

During the review, it was evident that researchers have also looked into issues where there is a limited view of information assets during asset identification. In addition, they have also overcome the limitation by suggesting other important assets in their papers. However, these researchers have suggested and discussed only one solution in each of their papers. All the non-technical factors which were discussed separately are compiled into a single frame. At the end of this analysis, it was possible to develop a taxonomy of technical and non-technical perspective during asset identification.

ISRA towards technical perspective assets: Each organization has to identify the risks to their most important assets and build a strategy for protecting its critical assets. Normally ISRA practitioners will examine which assets are most important to the organization in the early process of doing risk assessment. Based on the Stage 1 activities, the assets that will be considered first as important assets for an organization are listed in Fig. 3. In practical ISRA, practitioners will usually be targeting these assets as important assets for their organization when conducting risk assessments. This list of assets however, is subject to change whereby, it may increase or decrease based on the scope of security requirements of an organization (Fig. 3).

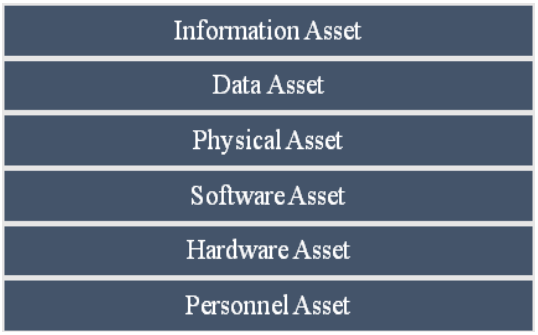

Fig. 3: List of important assets based on technical perspective

RESULTS AND DISCUSSION

ISRA towards non-technical perspective assets: Organizations have to revise the process of information security risk assessment by considering non-technical aspects rather than just the technical aspects. Since, traditional risk analysis has critical limitations where it adopts a more technical perspective, organizations must incorporate a business practice perspective into the identification of information security assets (Shedden *et al*., 2010). In other words, the term "information security assets" in a business practice perspective can refer to all assets other than technical asset (also known as non-technical assets). The types of a ssets that are categorized as non-technical perspective as sets by researcher shave been identified and scheduled as in Table 1.

Based on the Table 1 it can be concluded that many researchers have studied this issue separately. The results of the analysis indicate that there are two non-technical perspective as sets proposed by researchers to be prioritized during the risk identification process. These elements are knowledge and unofficial forms of information such as uncertified documents and unconsented release of information verbally or in written form. Some researchers had looked at this issue in isolation but to achieveefficient and effective information security, it is imperative toincorporate both non-technical assets aspects together. All views and suggestions given by the researchers are reviewed to identify the sub

Table 1: Analysis on non-technical perspective assets

Researchers	Knowledge	Unofficial form of information
Liu *et al*. (2006)	√	
Ahmad *et al*. (2005)	--	√
Shedden *et al*. (2010)	√	√
Shedden *et al*. (2011)	√	√
Bernard (2007)	--	√
Zakaria (2006)	√	--
Shedden *et al*. (2009)	√	--
Sanchez (2004)	√	--
Botha and Eloff (2001)	--	√
CISCO (2008a)	--	√
CISCO (2008b)	--	√
Fenz and Ekelhart (2009)	√	--
Belsis *et al*. (2005)	√	--
Choo (2000)	√	--

Compiled from relevant literature (Item Found = √)

elements liste dundereach of these two elements mentioned. Benefits derived from protecting the two elements are also reviewed.

Issues in knowledge: Knowledge is considered as the most strategically important resource and vital for organizations. Therefore, security analysts and practitioners required to have a broad knowledge of information security in order to efficiently apply general thinking strategies and confidently making effective decision regarding information security (Ben-Asher and Gonzalez, 2015; Souag *et al*., 2016). Knowledge can only be shared with others by deliberate actions. For instance tacit knowledge needs to be transferred to explicit knowledge in which information and knowledge need to be embedded in art efacts in order to make it understandable to others (Arnett and Wittmann, 2014). Therefore, organizations always request the experts to write-down or record information in publications, documentations, audio-visual materials, flowcharts, scripts, software code, procedures and so on in which their knowledge is articulated explicitly (Choo, 2000). The written documentation can provide a detailed description of how each task is to be performed, how long each task should take, the sequence of steps to be followed in performing each task and the steps that are to be taken by each worker in checking his or her own work.

The tacit knowledge usually relates to an understanding of their routine work's complexities and how it actually operates. It is very important to protect individually held tacit knowledge and explicit knowledge to ensure the ongoing availability of the organization's routine processes. People with experience and expertise are the organization's most vital information resource (Choo, 2000; Dane and Sonenshein, 2015) and they are considered as tacit knowledge of staffin the organization. They will help the organization perform its current tasks, transfer knowledge from one part of the organization to another and create new knowledge that may be useful to the organization (Sanchez, 2004). Shedden *et al*. (2011), says that the organization should identify the nature of individuals' and communities' critical knowledge as:

- Distributed knowledge (held collectively)
- Individually held tacit knowledge
- Individually held explicit knowledge

Organizations will be able to identify the key individual of the organization and also the critical knowledge held by the staff by taking into consideration the sub elements. In this respect, organizations would be able to identify the important people and their knowledge which is considered a significant driver not only of process efficiency and competitive advantage but also of accuracy in decision making that could lead to a greater availability of business processes and services. Thus, current ISRA should move from the method of identifying people as assets towards their availability to the organization and their individually-held and collective knowledge must also be identified for risk assessments (Shedden *et al*., 2009).

Issues in data and information assets: Securing information assets is a critical importance for organizations. Organizations continuously needs to invest in security endeavors even though all the information assets can be made absolutely secure and it may be prohibitively expensive (Nazareth and Choi, 2015). Therefore, currently available ISRA methods do profess that they cater for the protection of information assets and data assets to achieve a desired level of information security. Traditional ISRA methods have not listed the types of data and information that canbe consideredas an asset that must be protected. In addition, traditional ISRA methods have limitations in which they do not consider unofficial copies of assets or created unofficial assets by individual users that are defined and established through business practices (Ahmad *et al*., 2005; Shedden *et al*., 2011; Spears, 2006). Traditional ISRA methodologies only revealed formal and technical views of an organization's system or process (Shedden *et al*., 2010). Organizations are able to produce an accurate list of formal based documentation. However, the informal working environment occurs when employees violate the organization's formal processes and requirements. From an information security perspective, the informal organizational concept may unwittingly result in the leakage of information.

Every day we produce various kinds of formal and informal information that are to be treated as confiden tialand steps are to be taken to protect them from threats. Un official document lossor the probability to be achieved by the competi to rsis very high if the organization was lax and unconcerned with unofficial documents. It could lead to the loss of millions of dollars and customer trust will also be drastically affected. By getting to know all the unofficial information flow in organizations and the employees performing work around activities away from the formal view of the organization can help security staff

Table 2:Types of media commonly used

Media types	Example
Digital media	A form of electronic media where data are stored in digital form. Now a days data storage has started to shift from papers and files to computers and other paperless storage media Examples: Desktop PCs, notebook computer, Personal Digital Assistants (PDAs)
Physical media	Paper documents, e.g., information forms that can be written, printed and corresponded such as contracts, reports, drawings, production or transaction records and many other forms of paper data
Cognitive media	Exists in the minds of a personnel, eg., knowledge

to identify the correct assets by evaluating the specific risks to the firm. In addition, by listing out all the work around activities which lead to unofficial information flow could act as a guide to identify the actual assets used by the individuals in their day-to-day activities.

Based on Ahmad *et al*. (2005), information may exist on three types of media such as digital, physical and cognitive medias as shown in Table 2. Information has to flow through different organizational level and media to ensure the organization's operation continuity. Different people among the employees will create, store, distribute, transmit, access, use, maintain and destruct in performing their daily working activities. There are a variety of risks that can affect the confidentiality, integrity and availability of that information.

Ultimately, traditional ISRA methods are able to find official information flows and are also able to determine the formal state of the information flows. Conversely, information is leaked through employee's informal and unofficial workaround activities. There are legitimate reasons and processes for informal and unofficial information to exist or be created during the process of storage, distribution, transmission, access, use and destruction. Storage is the process of storing information in all of the places and in any form of media. Example: Saving or copying data/information to a data storage device. Distribution and transmission are processes performed by certain individuals in getting the information to locations where the information is available for use and is accessed by employees, very much depending on the nature of the process and whether they are official and/or unofficial activities. According to Eloff *et al*. (1996), all the information contained in documents represent the transaction based data of an organization. Documents are used as a vehicles for the exchange (distribute and transmittal) of information within, between and among organizations. The unofficial information will be created during the process of distribution and transmission of information. Example: Exchange of data/information either manual based documents or dynamic based documents within, between and among organizations. Access and use occur once information is accessible or available for use by employees which may also involve converting data from one media to another. Example: Activities such as printing, photocopying, capturing, scanning, typing, writing reading, hearing and speaking/discussing/ conversing. Destruction is the process of destroying information (digital, physical or cognitive media) when the information is no longer valuable or necessitated to be preserved Table 2. There will always be certain vulnerabilities existing in the staff's daily execution of activities. Therefore, it is important to find out all the possible ways of leakage of these information assets that can occur through their work practices.

New taxonomy of technical and non-technical perspective assets in ISRA's asset identification: Small or multi-national organizations need to determine which of the assets are most critical to the organization's success. Since risk and threats change over time, it is important that organizations periodically reassess risks and reconsider all of the important information-related assets. Organizations can conveniently identify all the important assets for their organization if there is a unanimously agreed common list of important assets to protect. Although organizations have a similar list ofcritical assets, the threat to theassetwillvary according to the scope of information security of theorganization. Thus, by having the list of important assets to be protected, organizations will be able to establish clear boundaries for the assets, identify its security requirements and cost effective controls (Shamala and Ahmad, 2014). Therefore, this paper contributes a new taxonomy of technical and non-technical perspective assets in ISRA's asset identification. ISRA practitioners can use the proposed taxonomy of assets to get a broader and clearer view for organization to access risk associated with these assets. The taxonomy can be used to a get clearer view of information assets which creates a strong basis for organizations to assess risk associated with those assets. As shown in Fig. 4, the new taxonomy has been developed.

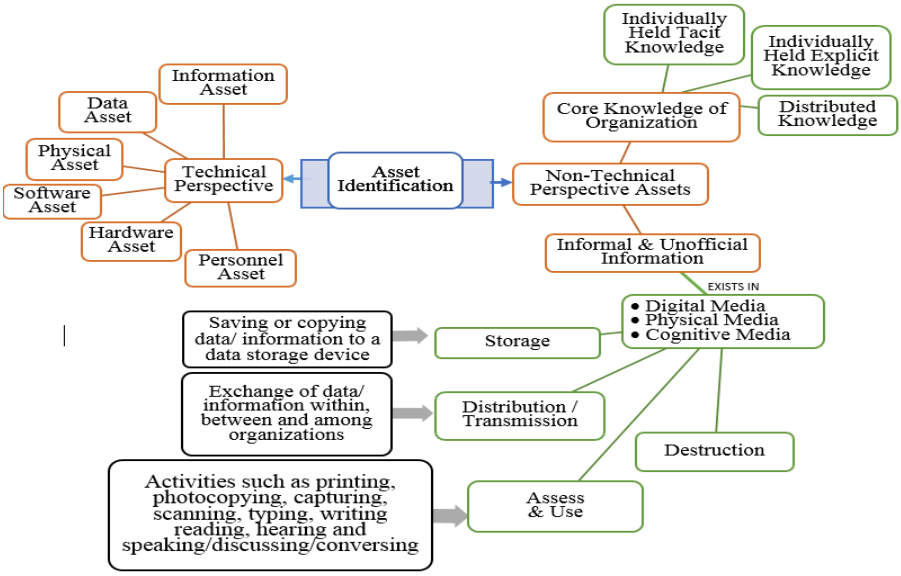

Fig. 4: Taxonomy of technical and non-technical perspective assets in ISRA's asset identification

CONCLUSION

The objectives of organizational ISRA which is to ensure the confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability can be delivered for key organizational informational assets, in a cost-effective manner. Generally, information assets in traditional ISRA are considered to be the infrastructural and informational elements that comprise information systems, including information assets, data assets, physical assets, software assets, hardware assets, personnel assets and people (Salmela, 2008; Shamala *et al*., 2013; Suh and Han, 2003).

Current traditional ISRA methods adopt a technical approach of identifying information assets while not considering people's knowledge which is known to be an important resource that is valuable for business continuity and formation of unofficial assets through informal workaround activities. Thus, the goal of the present study was focused on the development of taxonomy of technical and non-technical perspective assets which display all the assets through a socio-organizational and dynamic environment. This taxonomy is also able to present a complete view of an organization's assets which are deeply embedded within technical infrastructure, dynamic work environment and influence by user knowledge and formal and informal work environments. The taxonomy can guide practitioners to establish clear boundaries for the assets, identify its requirements and cost effective controls by having the list of important assets to be protected.

ACKNOWLEDGEMENTS

Researchers would like to thank Universiti Teknikal Malaysia Melaka (UTeM) and University Tun Hussien Onn Malaysia (UTHM) for supporting this research. This Research Funded by Minister of Higher Education under FRGS FRGS/2/2013/ICT07/ UTEM/02/1.

REFERENCES

Aagedal, J.O., F. den Braber, T. Dimitrakos, B.A. Gran, D. Raptis and K. Stolen, 2002. Model-based risk assessment to improve enterprise security. Proceedings of the 6th International Enterprise Distributed Object Computing Conference, September 17-20, 2002, Lausanne, Switzerland, pp: 51-62.

Ahmad, A., A.B. Ruighaver and W.T. Teo, 2005. An information-centric approach to data security in organizations. Proceedings of the IEEE Region 10 Conference, November 21-24, 2005, Melbourne, Australia -.

Alberts, C. and A.J. Dorofee, 2001. OCTAVESM criteria, version 2.0. Technical Report ESC-TR-2001-016, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA., USA., December 2001.

Alberts, C. and A.J. Dorofee, 2002. Managing Information Security Risks: The OCTAVESM Approach. Addison-Wesley Longman Publishing Co. Inc., Boston, MA., USA., ISBN-13: 9780321118868, Pages: 471.

Alberts, C., A. Dorofee, J. Stevens and C. Woody, 2003. Introduction to the OCTAVE® approach. Carnegie Mellon Software Engineering Institute, Pittsburgh, PA., USA., August 2003.

Alberts, C., A.J. Dorofee and J.H. Allen, 2001. OCTAVESM catalog of practices, version 2.0. Technical Report ESC-TR-2001-020, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA., USA., October 2001.

Alnatheer, M. and K. Nelson, 2009. A proposed framework for understanding information security culture and practices in the Saudi context. Proceedings of the 7th Australian Information Security Management Conference, December 1-3, 2009, Perth, Western Australia, pp: 6-17.

Arnett, D.B. and C.M. Wittmann, 2014. Improving marketing success: The role of tacit knowledge exchange between sales and marketing. J. Bus. Res., 67: 324-331.

Bandyopadhyay, K., P.P. Mykytyn and K. Mykytyn, 1999. A framework for integrated risk management in information technology. Manage. Decis., 37: 437-445.

Baskerville, R., 1991. Risk analysis as a source of professional knowledge. Comput. Secur., 10: 749-764.

Belsis, P., S. Kokolakis and E. Kiountouzis, 2005. Information systems security from a knowledge management perspective. Inform. Manage. Comput. Secur., 13: 189-202.

Ben-Asher, N. and C. Gonzalez, 2015. Effects of cyber security knowledge on attack detection. Comput. Hum. Behav., 48: 51-61.

Bernard, R., 2007. Information lifecycle security risk assessment: A tool for closing security gaps. Comput. Secur., 26: 26-30.

Bornman, W.G. and L. Labuschagne, 2004. A comparative framework for evaluating information security risk management methods. Proceedings of the Information Security South Africa Conference, June 30-July 1, 2004, Midrand, South Africa -.

Botha, R.A. and J.H.P. Eloff, 2001. Access control in document-centric workflow systems-an agent-based approach. Comput. Secur., 20: 525-532.

CISCO., 2008a. Data leakage worldwide: Common risks and mistakes employees make. CISCO Systems Inc., San Jose, CA., USA.

CISCO., 2008b. Data leakage worldwide: The high cost of insider threats. CISCO Systems Inc., San Jose, CA., USA.

Choo, C.W., 2000. Working with knowledge: How information professionals help organisations manage what they know? Library Manage., 21: 395-403.

Dahl, H.E.I., 2008. The CORAS method for security risk analysis. Proceedings of the 7th Estonian Summer School in Computer and Systems Science in cooperation with the Nordic Network on Dependable Systems, August 24-29, 2008, Otepaa, Estonia -.

Dane, E. and S. Sonenshein, 2015. On the role of experience in ethical decision making at work: An ethical expertise perspective. Organiz. Psychol. Rev., 5: 74-96.

Den Braber, F., I. Hogganvik, M.S. Lund, K. Stolen and F. Vraalsen, 2007. Model-based security analysis in seven steps-a guided tour to the CORAS method. BT Technol. J., 25: 101-117.

Dhillon, G. and J. Backhouse, 2001. Current directions in IS security research: Towards socio-organizational perspectives. Inf. Syst. J., 11: 127-153.

Elky, S., 2006. An introduction to information system risk management. SANS Institute, May 31, 2006. https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204.

Eloff, J.H., R. Holbein and S. Teufel, 1996. Security classification for documents. Comput. Secur., 15: 55-71.

Feng, N., H.J. Wang and M. Li, 2014. A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Inform. Sci., 256: 57-73.

Fenz, S. and A. Ekelhart, 2009. Formalizing information security knowledge. Proceedings of the 4th International Symposium on Information Computer and Communications Security ASIACCS 09 (2009), March 10-12, 2009, Sydney, Australia, pp: 183-194.

Fredriksen, R., M. Kristiansen, B.A. Gran, K. Stolen, T.A. Opperud and T. Dimitrakos, 2002. The CORAS framework for a model-based risk management process. Proceedings of the 21st International Conference on Computer Safety, Reliability and Security, September 10-13, 2002, Catania, Italy, pp: 94-105.

Gerber, M. and R. von Solms, 2005. Management of risk in the information age. Comput. Secur., 24: 16-30.

Halliday, S., K. Badenhorst and R. von Solms, 1996. A business approach to effective information technology risk analysis and management. Inform. Manage. Comput. Secur., 4: 19-31.

Jourdan, Z., R.K. Rainer Jr., T.E. Marshall and F.N. Ford, 2010. An investigation of organizational information security risk analysis. J. Serv. Sci., 3: 33-42.

Kailay, M. and P. Jarratt, 1995. RAMeX: A prototype expert system for computer security risk analysis and management. Comput. Secur., 14: 449-463.

Karabacak, B. and I. Sogukpinar, 2005. ISRAM: Information security risk analysis method. Comput. Secur., 24: 147-159.

Kolokotronis, N., C. Margaritis, P. Papadopoulou, P. Kanellis and D. Martakos, 2002. An integrated approach for securing electronic transactions over the web. Benchmarking: Int. J., 9: 166-181.

Liu, S., C. Cheung and L. Kwok, 2006. A knowledge framework for information security modeling. Proceedings of the 4th Australian Information Security Management Conference, December 5, 2006, Edith Cowan University, Perth, Western Australia -.

Lund, M.S., B. Solhaug and K. Stolen, 2011. A Guide Tour of the CORAS Method. In: Model-Driven Risk Analysis: The CORAS Approach, Lund, M.S., B. Solhaug and K. Stolen (Eds.). Chapter 3, Springer, Berlin, Germany, ISBN-13: 9783642123238, pp: 23-43.

NIST., 2010. Guide for applying the risk management framework to federal information systems. Joint Task Force Transformation Initiative, Special Publication 800-37, Revision 1, NIST, Gaithersburg, MD., USA.

NIST., 2011. Managing information security risk: Organization, mission and information system view. NIST Special Publication 800-39, National Institute of Standards and Technology, Gaithersburg, MD., USA., March 2011.

NIST., 2012. Guide for conducting risk assessments: Information security. NIST Special Publication 800-30 (Revision 1), National Institute of Standards and Technology, Gaithersburg, MD., USA., September 2012.

Nazareth, D.L. and J. Choi, 2015. A system dynamics model for information security management. Inform. Manage., 52: 123-134.

Onwubiko, C. and A.P. Lenaghan, 2007. Managing security threats and vulnerabilities for small to medium enterprises. Proceedings of the IEEE Conference on Intelligence and Security Informatics, May 23-24, 2007, New Jersey, pp: 244-249.

Rainer, Jr. R.K., C.A. Snyder and H.H. Carr, 1991. Risk analysis for information technology. J. Manage. Inform. Syst., 8: 129-147.

Ramli, N.A. and N.A. Aziz, 2012. Risk identification for an information security management system implementation. Proceedings of the 6th International Conference on Emerging Security Information, Systems and Technologies, August 19-24, 2012, Rome, Italy, pp: 57-61.

Raymond, K., 1995. Reference Model of Open Distributed Processing (RM-ODP): Introduction. In: Open Distributed Processing, Raymond, K. and L. Armstrong (Eds.). Chapter 1, Springer, USA., ISBN: 978-1-4757-6074-3, pp: 3-14.

Refsdal, A., 2011a. Analysing risk in practice: The CORAS approach to model-driven risk analysis. Proceedings of the 18th ACM Conference on Computer and Communications Security, October 17-21, 2011, Chicago, IL., USA -.

Refsdal, A., 2011b. The CORAS approach to model-driven risk analysis. Proceedings of the e-RISE 2011 Workshop: Engineering of Risk and Security Requirements, May 13, 2011, Dauphine University, Paris, France -.

Richardson, R., 2008. 2008 CSI computer crime and security survey. Computer Security Institute, New York. http://www.kwell.net/doc/FBI2008.pdf.

Siemens, 2005. Managing CRAMM reviews using PRINCE. SIEMENS Enterprise, Erlangen, Germany.

Salmela, H., 2008. Analysing business losses caused by information systems risk: A business process analysis approach. J. Inform. Technol., 23: 185-202.

Sanchez, R., 2004. Tacit knowledge versus explicit knowledge approaches to knowledge management practice. http://www.fraserhealth.ca/media/Tacit-vs-Explicit%20Knowledge%20Transfer.pdf.

Sarkheyli, A. and N.B. Ithnin, 2010. Improving the current risk analysis techniques by study of their process and using the human body's immune system. Proceedings of the 5th International Symposium on Telecommunications, December 4-6, 2010, Tehran, Iran, pp: 651-656.

Shamala, P. and R. Ahmad, 2014. A proposed taxonomy of assets for Information Security Risk Assessment (ISRA). Proceedings of the 4th World Congress on Information and Communication Technologies, December 8-11, 2014, Bandar Hilir, Malacca, Malaysia, pp: 29-33.

Shamala, P., R. Ahmad and M. Yusoff, 2013. A conceptual framework of info structure for Information Security Risk Assessment (ISRA). J. Inform. Secur. Applic., 18: 45-52.

Shedden, P., R. Scheepers, W. Smith and A. Ahmad, 2011. Incorporating a knowledge perspective into security risk assessments. Vine, 41: 152-166.

Shedden, P., W. Smith and A. Ahmad, 2010. Information security risk assessment: Towards a business practice perspective. Proceedings of the 8th Australian Information Security Management Conference, November 30-December 2, 2010, Perth, Australia, pp: 119-130.

Shedden, P., W. Smith, R. Scheepers and A. Ahmad, 2009. Towards a knowledge perspective in information security risk assessments-an illustrative case study.

Proceedings of the 20th Australasian Conference on Information Systems, December 2-4, 2009, Melbourne, Australia, pp: 74-84.

Souag, A., R. Mazo, C. Salinesi and I. Comyn-Wattiau, 2016. Reusable knowledge in security requirements engineering: A systematic mapping study. Requir. Eng., 21: 251-283.

Spears, J.L., 2006. A Holistic Risk Analysis Method for Identifying Information Security Risks. In: Security Management, Integrity and Internal Control in Information Systems, Dowland, P., S. Furnell, B. Thuraisingham and X.S. Wang (Eds.). Springer, Boston, MA., USA., ISBN: 978-0-387-29826-9, pp: 185-202.

Stolen, K., F. den Braber, T. Dimitrakos, R. Fredriksen and B.A. Gran et al., 2002. Model-based risk assessment-the coras approach. Proceedings of the 1st iTrust Workshop on Trust Management in Dynamic Open Systems, September 2-4, Glasgow, UK.

Stoneburner, G., A. Goguen and A. Feringa, 2002. Risk management guide for information technology systems. NIST Special Publication 800-30, National Institute of Standards and Technology, Gaithersburg, MD., USA., July 2002.

Suh, B. and I. Han, 2003. The IS risk analysis based on a business model. Inform. Manage., 41: 149-158.

Syalim, A., Y. Hori and K. Sakurai, 2009. Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. Proceedings of the International Conference on Availability, Reliability and Security, March 16-19, 2009, Fukuoka, Japan, pp: 726-731.

Visintine, V., 2003. An introduction to information risk assessment. GSEC Practical, Version 1.4b, SANS Institute, USA., August 8, 2003.

Vorster, A. and L.E.S. Labuschagne, 2005. A framework for comparing different information security risk analysis methodologies. Proceedings of the Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries, September 20-22, 2005, South Africa, pp: 95-103.

Webster, J. and R.T. Watson, 2002. Analyzing the past to prepare for the future: Writing a literature review. MIS Q., 26: 12-22.

Yazar, Z., 2002. A qualitative risk analysis and management tool-CRAMM. Version 1.3, SANS Institute, USA.

Zakaria, O., 2006. Internalisation of information security culture amongst employees through basic security knowledge. Proceedings of the IFIP TC-11 21st International Information Security Conference, May 22-24, 2006, Karlstad, Sweden, pp: 437-441.