THE RELATIONSHIP BETWEEN INFORMATION SYSTEMS RESOURCES AND INFORMATION SECURITY

Norizan Anwar[1]*, Mohamad Noorman Masrek[2], Muhamad Khairulnizam Zaini[3] and Qamarul Nazrin Harun[4]

[1]Senior Lecturer, Universiti Teknologi MARA, Malaysia, norizananwar@gmail.com
[2]Assoc. Prof. Dr., Universiti Teknologi MARA, Malaysia, mnoormanm@gmail.com
[3]Lecturer, Universiti Teknologi MARA, Malaysia, nizam0374@salam.uitm.edu.my
[4]Master Student, Universiti Teknologi MARA, Malaysia, qamarulnaz@gmail.com
*Corresponding author

Abstract

Information is an asset crucial for the survival of any organizations. Because of its importance, information needs to be safeguarded and protected, normally termed as information security. The ISO 27001:2005 defines information security as “the preservation of confidentiality, integrity and availability of information”. Hence, information security is designed to protect the valuable data of the organization and it is importance in safe-guarding all organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity. Realizing the importance of information security, researchers have studied and proposed various models for an effective implementation of information security. To further adds to this body of literature, this paper reports the findings of a study examining information systems resources and its effect on information security. Using the survey research method with questionnaire as the instrument for data collection, a total of 72 companies located in Klang Valley and Cyberjaya, Malayaia were engaged in the study. The findings suggest that, several dimensions of information systems resources are significant predictor of information security. The findings should be useful to both researchers and practitioners. As for the researchers, the model used can be further tested in other settings, while for the practitioners, it provides a useful guideline for improving their information systems infrastructure so as to protect and safeguard their organizational information.

Keywords: Information Security, Information Technology (IT) Resources, Relationship Resources, Information Security Infrastructure, IT Department Characteristics, MSC Status Companies, SPSS.

1. INTRODUCTION

No matter how small or large the organization are, the security of the information must be given priority so as to protect all of the organization information including product information, financial information, customer information, supplier information, human resource information etc. Failing to establish proper information security will endanger the organizations to various threats, coming not only from external sources but also

internal sources, who are normally the employees of the organization itself. Infosec Institute (2014) reported that, threats originating from internal sources were considered as one of the most significant risks to the overall security of any organization. The study revealed that 37% ex-employee had caused fraud towards their former organization, 21% of ex-employees had caused IT sabotage, 19% of ex-employees had espionage the classified information, 15% of employees had caused Intellectual Property (IP) theft incident and 8% are others insider threat. On the other hand, threats caused by external sources are also equally dangerous. Price Water House Coopers (2015) noted 10% of the outsider threats are from terrorists; 15% are organized crime that intentionally planned; 16% are from activist organizations or hacktivists; 16% information brokers which violates the organization's security systems in order to gain the confidential information; 24% are from their competitors; 9% are from foreign entities and organizations; 7% are from foreign nation-states; 6% are from domestic intelligence service; 24% of outsider threats are from hackers and 18% of outsider threats are unknown.

Realizing the importance of information security, researchers have studied and proposed various models for an effective implementation of information security. Most of these studies are either focusing on technical aspects or non-technical aspects. Within the breadth of technical aspects, past studies mainly concerned on the technical implementations such as installation of firewalls, IDS, antivirus and etc. On the other hand, as for the non-technical aspects, the information security culture has been the dominant topic addressed by most previous studies (e.g. Da Veiga, 2016). Chang & Wang (2010) adopted a different approach and focused on the information systems infrastructure as the determinant of successful implementation of information security. Given the uniqueness of this study, the researcher felt it would be an interesting endeavor to further test their model. Accordingly, a study was undertaken with the aim of (i) validating the Chang & Wang (2010) model in the context of Malaysia (ii) to identify the status of information systems resources of the participating organizations and (iii) the identify the level of the perceived information security of the participating organizations.

2. LITERATURE REVIEW

2.1 Overview of Information Security

Information security has been defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability". Hong et al. (2006) as cited by Singh, Gupta and Ojha (2014), described information security as "the application of methodological and managerial processes on the information hardware, software, and data that can help in keeping organizational assets and personal privacy protected". Hence, information security is a discipline that helps to alleviate the risk of information via physical, technical, or operational of security controls.

Alavi, Islam & Mouratidis (2016) stated that information security, as part of corporate governance, assists organisations to achieve greater productivity with better cost efficiencies as well as legal and regulatory compliance. However, information security is often seen as a remote activity by many organisations with a technical nature. Therefore, they fail to link business objectives to security goals. (Ahmad & Maynard, 2014) stated that "managing organizational information security needs the application of a range of formal, informal, and technical security controls to address multifaceted security risks". In addition to excellent management skills, information security managers need to understand of how security supports business objectives, as well as a broad working knowledge of several security practices.

The literature shows that, there are many predictors of information security. Among them are controls (administrative controls, logical controls, and physical controls) (Feruza & Kim, 2007); security policy, organizational culture, and human behavior actions (Imam & Hammoud, 2014); organizational and national cultural values, and the implementation of the associated technology (Alfawaz, 2011); IT literacy, IT policies, top management commitment, and organization's resources (Ngura, Kimwele & Rotich, 2015); information security policy (Al-Awadi & Renaud, 2007); information system resources (Chang & Wang, 2010). The study by Chang & Wang (2010) operationalized information system resources as comprising of IT resources, relationship resources, and information security infrastructure. Their study found that these three dimensions of information system resources (ISR) significant predictors of information security.

2.2 Information Systems Resources

The term 'information systems' is usually defined as a combination of hardware, software, people, procedure and data. Computer based information systems is used for data processing and delivering information. Drawing upon this background, information systems resources (ISR) is referred as the information infrastructure comprising all IT components including hardware, software as well as the processes and

procedures that governs the use of all computer-based information systems. Nowadays, ISR is no longer considered lavish investment but a necessity that must be implemented by all business organizations. According to Chang & Wang (2010), ISR is "essential for organizations to have a variety of IS resources to thwart the potential threats caused by the system breaches". ISR consists of several components that can prevent and secure the organization resources from their enemies. Earlier study by Ross, Beath & Goodhue (1996) operationalized ISR as having three elements of IT assets which are human assets, technology assets, and relationship assets. Subsequently, Chang & Wang (2010) extended the ISR measurements as comprising of information technology resources (ITR), relationship resources (RR), and IS infrastructure resources (IIS).

3. THEORETICAL FRAMEWORK

Fig. 1 shows the theoretical framework of the study. The framework was adapted from Chang & Wang (2010), who developed the framework based on the work of Byrd & Turner (2000), Ravichandran & Lertwongsatien (2005), and Lee et al. (2004). The ISR comprising of IT resources, relationship resources and information security infrastructure are hypothesized to be a significant predictors of information security.

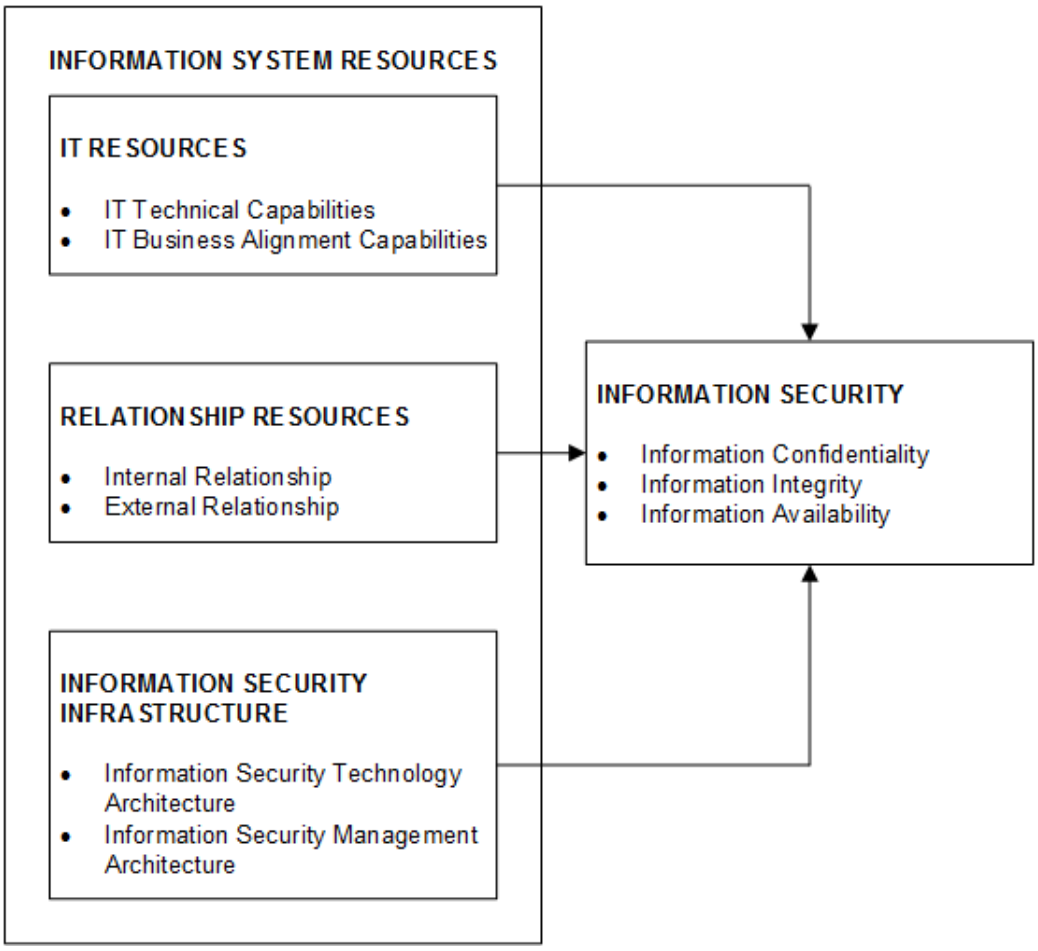

Fig. 1: Theoretical Framework

3.1. IT Resources

IT resources react as tools to an organization to operate their business operation. IT resources is about soft skills, tangible and intangible capabilities, knowledge, and skills. Chang & Wang (2010) defined IT resources as an IS personnel knowledge and skills about IT related matters. Moreover, IT resources should also include software, hardware, communications, IT applications and IT personnel (Shih & Wen, 2003). There are five attributes of IT resources highlighted by Mata et al. (1995) in their study which are customer switching costs, access to capital, proprietary technology, technical IT skills, and managerial IT skills. For better business performance, to support business organization function, internal and external

communication, organizations should ensure their IT resources works effectively, efficiently and in accordingly. Above all, IT resources in organization claim to be important in conceiving new IT applications, developing and testing new IT applications, implementing new IT applications, and day-to-day operation of IT applications. In measuring IT resources, there are two (2) dimensions is use which is IT technical capabilities and IT business alignment capabilities. IT technical capabilities are more on the IT/IS personnel technical knowledge and skills. Among IT/IS personnel, this technical knowledge and skills is important for them to response to any circumstances and unexpected situation in quick response rate. Thereby, the operation of the business operation can continue by less than a day. In regards to the contingency situation, the IT/IS personnel is capable to operate and maintain any IS interruption or break down (Henderson & Venkatraman, 1993). Meanwhile, IT business alignment capabilities are about how organizations align between their IT capabilities with business strategy by using in-house IT/IS personnel knowledge and skills available (Lee, Trauth & Farwell, 1995). Hiring the right, eligible, and appropriate IT/IS personnel is not only letting them to support basic IT stuff much more, i.e. ensuring the IT infrastructure of the organization is secure, re-align the IT infrastructure to any changes in customers or market demands besides of planning new strategy. The IT/IS personnel could prevent and prepare the right shield in protecting all organization resources from unwanted visitors. In essence, by seeing the important of IT resources to the information security, the hypothesis of the study is:

H1: IT Resources is significantly related to Information Security.

3.2. Relationship Resources

An organization required no communication breakdown whether internally or externally in running their day-to-day activities. A good communication will enable the organization smooth sailing any transaction made between customers, suppliers and vendors. Due to that, related mechanisms and protocols should in place in the organization IT infrastructure. Initially, relationship resources is about the organization linkages with their internal or external clients. Hence, the relationship may be come from whether internal or/and external any of the organization. Internal relationship may involve between departments while external relationship may with suppliers or customers. Even though, a good relationship should exist between them, not all data, information, and documents can be easily share. The organization should identify the level or limitation to what extent the data, information, and documents can be transferred between them. In conjunction to that, the organization should evaluate which part of the business process they may allow the transfer and sharing activities (Johnson & Eric, 2007). Therefore the hypothesis of the relationship resource factors in this study is:

H2: Relationship Resources is significantly related to Information Security

3.3. Information Security Infrastructure

Policies and/or standard operating procedure (SOP) on information security should exist and well practice in order to assist the organization to monitor the implementation. For example in Japan, the implementation shows that the government will responsible to highlight policies for the promotion of strategies concerning information security technology, protection and redemption of rights and benefits, crime control, promotion of international partnership and cooperation, and developing and ensuring human resources engaged in information security (Nisc's Web site, 2008). Meanwhile in India, Ranjan et al. (2012) in their study highlight that the most prominent role and body in fulfilling and developing the policies is produced by their National IT Policy and the National Cyber Security Policy. The content of this policy is basically all about the needs for secure, robust and scalable IT components in its infrastructure on top of having good Information Security Infrastructure. Information security infrastructure is about having secure IT environment in the organization from the cyber attacks. Study by Byrd, Lewis & Turner (2004) indicates that the development of information security technical architecture is influencing the information security. Additional factor that also influence information security is the management side, i.e. information security management architecture (Chang & Ho, 2006). Information security technology architecture refers to these two information systems components that are software and hardware. Meanwhile, Information security management architecture refers to organizations that manage and control the security of information systems via published and circulation of their rules and regulations within and without organizations. Due to the above statement, the hypothesis of Information security infrastructure factors is:

H3: Information Security Infrastructure is significantly related to Information Security

4. METHODOLOGY

4.1. Research Approach

In terms of approach, this research is considered as quantitative. According to Burns & Grove (2005) quantitative research is a formal, objective, systematic process in which numerical data are used to obtain information about the world. The method employed in this study is survey, which is defined as as a method that consists of selecting a sample of respondents and administering a standardized questionnaire to them.

4.2. Instrument and Method

The instrument used for collecting the data was questionnaire. Sekaran (2003) mentioned that a researcher should adopt a well validated and reliable measures to ensure that the research is scientific and escape the laborious efforts in developing a new measure. Following the advice from Sekaran (2003), the instrument was developed based on the work of Chang & Wang (2010). Prior to the actual data collection, the instrument was pre-tested and pilot tested with 72 respondents. All measures for the variables shown in Fig. 1 were using Likert Scale anchored with five option with 1 for “Strongly Disagree”, 2 for “Disagree”, 3 for “Undecided / Neutral”, 4 for “Agree” and 5 for “Strongly Agree”. Overall, there are altogether 56 items used in the questionnaire. Prior to the actual data collection, the questionnaire underwent rigorous pre-testing and pilot testing so as to ensure that study produced valid and reliable results.

4.3. Population and Sampling

As the unit of analysis of the study is firm level, hence, the researchers had to decide the appropriate companies to be engaged in this study. However, important criteria to qualify for the study is that the company must be heavily employed ICT for doing their business. After careful consideration, the MSC status companies located within the vicinity of CyberCity and CyberCentre were chosen as they fulfill the required criteria. Due to time and other constraints, the study had to limit to only 150 companies as the targeted respondents. Accordingly, using the simple random sampling technique, 150 questionnaires were sent out to these companies. A total of 119 were returned and upon further scrutiny on the returned questionnaire, 47 had to be removed because they were information security were not fully implemented in these organizations.

5. RESULTS

5.1. Demographic Profile of Respondents

Table 1 presents the demographic profile of the respondents. Out of 72 respondents, 1.4% were Creative Multimedia, 1.61% were Software Development, 51.61% were Support Services, 12.90% were Hardware Design, 16.13% were Internet Based Business and 14.52% were Shared Service and Outsources (SSO). However, number of staff in company, the highest percentage was less than 200 staff and while the lowers percentage is between 801 to 1000 staff. With the regard to respondents’ position, the highest percentage i.e. 32.39% indicated that they were executives while the lowest which was 2.82% each indicated that they were assistance managers and non-executives. Majority of the respondents’ i.e. 62.50% indicated that their number of staff in IT department is only 1.

Table 1: Demographic Profile of Respondents

Characteristics	Items	Frequency	Percentage
Company sector	Creative Multimedia	1	1.61%
	Software Development	32	51.61%
	Support Services	8	12.90%
	Hardware Design	2	3.23%
	Internet Based Business	10	16.13%
	Shared Services and Outsourcing	9	14.52%

Characteristics	Items	Frequency	Percentage
Number of staff in company	Less than 200	57	79.17%
	201 – 400	5	6.94%
	401 – 600	3	4.17%
	601 – 800	0	0.00%
	801 – 1000	1	1.39%
	More than 1000	6	8.33%
Position	General Manager	3	4.23%
	Head of Department	3	4.23%
	Senior Manager/ Manager	9	12.68%
	Assistance Manager	2	2.82%
	Senior Executive	7	9.86%
	Executive	23	32.39%
	Non Executive	2	2.82%
	Others	22	30.99%
Number of staff in IT Department	1	40	62.50%
	2	7	10.94%
	3	5	7.81%
	4	5	7.81%
	6	7	10.94%

5.2. Reliability Analysis

Reliability analysis was performed to determine the scale's internal consistency strength. The results as shown in Table 2 indicated that all variables are above the recommended cut-off value which is 0.7 (Nunally & Bernstein, 1994), hence suggesting that the scale used in the study was highly reliable.

Table 2: Realibility Analysis of Research Variable/Dimensions

Variable	**No. of Items**	**Cronbach's Alpha**
Information Security	11	0.944
IT Resources		
IT Technical Capabilities	8	0.872

IT Business Alignment Capabilities	6	0.928
Relationship Resources		
Internal Relationship	5	0.908
External Relationship	4	0.892
Information Security Infrastructure		
Information Security Technology Architecture	7	0.959
Information Security Management Architecture	7	0.951

5.3. Descriptive Analysis

Table 3 exhibits the descriptive analysis of every each variable and dimension measures in the current study. The results show that the mean value of information security is at 4.1701 which represents agree among the responses where the Likert scale use is between 1 for “Strongly Disagree” to 5 for “Strongly Agree”. This scale is use consistently across all items in the study. Looking at the first factor of information security, i.e. IT resources, the dimension of IT Technical Capabilities indicate that the mean value is almost to agree. The responses of among MSC status company feels that their IT personnel should equipped with related technical skills such as multiple programming language, systems analysis and design, operating IS, maintaining IS, and diagnose any IS problems. For the second dimension is IT Business Alignment Capabilities, the level of responses is same as previous dimension. The organization looking seriously the capabilities of IT personnel in aligning the IT investment with long-term business needs, developing the technical solutions for business problems solving, aligning the IT strategy with the organization’s strategy, and understanding on business environment, goals, and plans. In the perspective of Relationship Resources, there are two dimensions which are internal relationship and external relationship respectively. Both relationship depict the level of agree among those responses. This indicates that MSC status company concern and aware to what extent the communication and relationship should exist between them. Within internal relationship, the staffs are understand each department working environment, build in trust within each other, the conflicts between department is rarely happen, one another department is working closely together, and if there is any conflicts between department, they are able to solve through mutual adjustment and communications. Meanwhile for the external relationship, their practice is only share related information, respond to any information require in a timely manner, build trust, and they also have a good relationship between the organizations and business partners (i.e. suppliers and customers). The last factor that measure information security is Information Security Infrastructure. Both dimensions, i.e. Information Security Technology Architecture and Information Security Management Architecture shows that the responses of MSC status company is at agree level. It is seen that the MSC status company is taking care and ensure that their infrastructure especially at their information security technology architecture is within control, such the software and hardware is effectively control network security, user access rights, data access, encrypt or decrypt data, store data, prevent malicious intrusion, and generate log analysis reports. The management level of information security architecture shows that these organization is cater the (1) information security objectives, (2) the responsibility for information user, (3) the process of managing security events, (4) information systems development, and (4) information systems maintenance is well defined, (5) the use of information property is well regulated, and (6) the continuity of systems operation is well managed. As overall level of the research, the responses are agree with the variables and dimensions use.

Table 3: Descriptive Analysis of Research Variables/Dimensions

Variable / Dimension	Mean	Std. Deviation	Variance	Minimum	Maximum
Information Security	4.1701	0.68064	0.463	1.82	5.00
IT Resources					
IT Technical Capabilities	3.8339	0.68720	0.470	1.00	5.00
IT Business Alignment Capabilities	4.0751	0.68994	0.476	1.67	5.00
Relationship Resources					
Internal Relationship	4.0620	0.74342	0.553	1.00	5.00
External Relationship	3.9859	0.73301	0.537	1.00	5.00
Information Security Infrastructure					
Information Security Technology Architecture	4.0612	0.80979	0.656	1.14	5.00
Information Security Management Architecture	3.9265	0.76012	0.578	1.29	5.00
Overall	**4.0164**	**0.72916**	**0.533**	**1.15**	**5.00**

5.4. Correlation Analysis

As illustrated in Table 4, the results suggest that the values of Pearson correlation are between 0.695 and 0.839. Wong & Hiew (2005) noted that value above between 0.5 and 1.0 is considered strong relationship. As all the Pearson correlation values are less than 0.9, hence suggesting that the variables are not experiencing the problem of multicollinearity.

Table 4: Correlation Analysis Amongst Research Variables

Variables	ISec	ITR	RR	ISI
Information Security (ISec)	1			
IT Resources (ITR)	0.790	1		
Relationship Resources (RR)	0.695	0.791	1	
Information Security Infrastructure (ISI)	0.839	0.798	0.727	1

5.5. Regression Analysis (Hypothesis Testing)

Table 5 and 6 present the results of the multiple regression analysis. As shown in Table 6, R square recorded a value of 0.744, hence implying that 74.4% variance in ISRIS can be explained by the combination of the independent variables which are IT Resources, Relationship Resources, and Information Security Infrastructure.

Table 5: Model Summary of Regression Analysis Between Independent Variables and Dependent Variables

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.863[a]	0.744	0.732	0.35353
a. Predictors: (Constant), IT Resources, Relationship Resources, Information Security Infrastructure				
b. Dependent Variable: Information Security				

Upon further scrutiny of the results showed that, out of the three investigated independent variables, only two turned out to be influential in predicting Information Security. These variables were IT Resources ($t = 2.517$, $p < 0.05$), and Information Security Infrastructure ($t = 5.174$, $p < 0.05$) (Refer to Table 6).

Table 6: Coefficient Table for Variables Predicting Information Security

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.631	0.285		2.214	0.030
	IT Resources	0.336	0.133	0.307	2.517	0.014
	Relationship Resources	0.044	0.109	0.043	0.401	0.690
	Information Security Infrastructure	0.509	0.098	0.562	5.174	0.000
a. Dependent Variable: Information Security						

6. DISCUSSION

The conduct of this study has been to investigate factors that influence ISRIS among MSC status companies. To achieve the objective, an empirical based framework consisting three independent variables which are IT Resources, Relationship Resources and Information Security Infrastructure; and one dependent variable i.e. Information Security has been adopted. Based on the analyses of the collected data, only two variables were found to be relevant in determining Information Security. Specifically, the variables are IT Resources and Information Security Infrastructure which is contributing about 74.4% variance in Information Security. In this study, the results of the finding is somewhat contradict with the original study of which the framework was adopted i.e. Chang & Wang (2010). In their study, all the independent variables were found to be a significant predictor of information security. However, in this study, the relationship resources were found to be insignificant predictors. One plausible explanation to this finding is that the sample size used in this study was relatively small as compared to the study of Chang & Wang (2010).

7. CONCLUSION

Researchers who are interested to further explore the topic may consider adopting the model to be tested in other organization settings. Perhaps, the developed framework can be further tested in other Information Security settings. From the practical viewpoint, the instrument that had been developed in this study could be used by the any organization to gauge their performance in terms of imposed security policies and

management the relationship between Information Security itself. Just as in other study, this study is not without limitation. The first limitation is in terms of the number of respondents is less than 100 and shall cover more MSC Malaysia Cybercity and Cybercentre. Further study should consider employing more respondents and area of study. In addition, besides using the survey research method, studies adopting qualitative or mixed method will provide richer and deeper understanding on factors that drive organization towards the relationship between Information Security.

8. ACKNOWLEDGEMENT

This research was funded by the Research Management Institute (RMI), Universiti Teknologi MARA (UiTM) and Faculty of Information Management, Puncak Perdana Campus.

REFERENCE LIST

Ahmad, A. & Maynard, S. (2014). Teaching information security management: reflections and experience. Information Management & Security, 22(5), 513-536.

Alavi, R., Islam, S. & Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. Information & Computer Security, 24(2), 205-227.

Al-Awadi, M. & Renaud, K. (2007). Success factors in information security implementation in organizations. 2007 IADIS International Conference e-Society.

Alfawaz, S. M. (2011). Information security management: A case study of an information security culture. Retrieved from Queensland University Of Technology Digital Dissertation. (41777)

Burns, N. & Grove, S. K. (2005). The Practice of Nursing Research: Conduct, Critique, and Utilization (5th Ed.). St. Louis, Elsevier Saunders.

Byrd, T. A., Lewis, B. R. & Turner, D. E. (2004) The impact of IT personnel skills on IS infrastructure and competitive IS. Information Resources Management Journal, 17(2), 38-62.

Byrd, T. A. & Turner, D. E. (2000). Measuring the flexibility of information technology infrastructure: exploratory analysis of a construct. Journal of Management Information Systems, 17(1), 167–208.

Chang, K-C. & Wang, C-P. (2010). Information systems resources and information security. Journal of Information Systems Frontiers, 1-15.

Chang, S. E. & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345– 361.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: illustrated through an empirical study. *Information & Computer. Security*, *24*(2), 139–151.

Feruza Y., S. & Kim, T-H. (2007). IT security review: Privacy, protection, access control, assurance and system security. International Journal of Multimedia and Ubiquitous Engineering, 2 (2), 17-32.

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: leveraging information technology for transforming organizations. IBM Systems Journal, 38(2), 472–484.

Imam, A. H. & Hammoud, M. S. (2014). The impact of non-technical security management factors on information security management in health informatics. International Journal of Information Technology and Business Management, 26 (1), 13-28.

InfoSec Institute (2014). *2013 data breaches: all you need to know*. Retrieved from http://resources.infosecinstitute.com/2013-data-breaches-need-know/

Johnson ,M. E. & Eric, G. (2007). Managing Organizational Security: Embedding Information Security into the Organization. Retrieved at www.computer.org/security/ on 14 August 2011.

Kissel, R. (2011). Glossary of Key Information Security Terms. National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

Lee, D. M. S., Trauth, E. & Farwell, D. (1995). Critical skills and knowledge requirements of IS professionals:

a joint academic/ industry investigation. MIS Quarterly, 19(3), 313-340.

Lee, Y. W., et al. (2004). Process-embedded data integrity. Journal of Database Management, 15(1), 87–103.

Mata, F. J., Fuerst, W. L. & Barney, J. B. (1995). Information technology and sustained competitive advantage: a resource- based analysis. MIS Quarterly, 19(4), 487–505.

Ngura, S., Kimwele, M. & Rotich, G. (2015). Determinants of information security among small and medium enterprises in Kenya, European Journal of Business Management, 2 (1), 1-20.

Nunnally, B. S. & Berstein, I. H. (1994). Psychometric theory (3rd Ed.). New York: McGrawHill.

Price Water House Coopers International Limited. (2015). *Managing cyber risks in an interconnected world*.

Ranjan, S., Maurya, M. K., Malviya, A. K., Yadav, R., Gupta, R., Mishra, M. & Rai, S. (2012). Building an Information Security Infrastructure - A Comprehensive Framework towards a Robust, Resilient and Dependable Infrastructure. International Journal of Computer Science Issues, 9 (3), 414 - 419.

Ross, J. W., Beath, C. M., & Goodhue, D. L. (1996). Develop Long-term Competitiveness Through IT Assets. Sloan Management Review, 38 (1), 31-42.

Ravichandran, T. & Lertwongsatien, C. (2005). Effect of information systems resources and capabilities on firm performance: a resource-based perspective. Journal of Management Information Systems, 21(4), 237–276.

Sekaran, U. (2003). Research methods for business: a skill building approach. Fourth edition. Singapore: John Wiley and Sons.

Shih, S. C., & Wen, H. J. (2003). Building e-enterprise security: a business view. Information System Security, 12(4), 41–49.

Singh, A.N. Gupta, M.P. & Ojha, A. (2014). Identifying factors or organizational information security. Enterprise Information Management, 27(5), 644-667.

Wang, A. J. A., Xia, M. & Zhang, F. (2008). Metrics for information security vulnerabilities. Journal of Applied Global Research, 1 (1), 48-58.

Wong, C. C. & Hiew, P. L. (2005). Diffusion of mobile entertainment in Malaysia: drivers and barriers. Enformika, 5, 263-266.

(2008). Intensive Efforts for Enhancing Information Security Infrastructure. Information Security Policy Council. Retrieved from World Wide Web http://www.nisc.go.jp/eng/pdf/sj2008_eng.pdf on 1 November 2012.