International Journal of Business and Society, Vol.21 No.3, 2020, 1203-1214

EXAMINING THE RELATIONSHIP BETWEEN INFORMATION SECURITY EFFECTIVENESS AND INFORMATION SECURITY THREATS

Mohamad Noorman Masrek[♣]
Universiti Teknologi MARA Selangor

Tri Soesantari
Universitas Airlangga

Asad Khan
University of Peshawar

Aang Kisnu Dermawan
Universitas Islam Madura

ABSTRACT

Information is the most critical asset of any organizations and business. It is considered as the lifeblood of the organization or business. Because of its importance, information needs to be protected and safeguarded from any forms of threats and this is termed as information security. Information security policy and procedure has been regarded as one of the most important controls and measures for information security. A well-developed information security policy and procedure will ensure that information is kept safe form any harms and threats. The aim of this study is to examine the relationship between information security policy effectiveness and information security threats. 292 federal government agencies were surveyed in terms of their and information security practices and the threats that they had experienced. Based on the collected, an analysis using partial least square structural equation modeling (PLS-SEM) was performed and the results showed that there is a significant relationship between information security policy effectiveness and information security threats. The finding provides empirical evidence on the importance of developing an effective information security policy and procedure.

Keywords: *information security, security policy, information threats, structural equation modelling, survey, Malaysia*

Received: 9 July 2019
Accepted: 14 September 2020

1. INTRODUCTION

Information is the most critical asset of any organizations and business. It is considered as the lifeblood of the organization or business and because of its importance, information needs to be

♣ Corresponding author: Faculty of Information Management, Universiti Teknologi MARA Selangor, Kampus Puncak Perdana, Seksyen U10, 40150 Shah Alam Selangor Malaysia. Telephone: +60379622134. E-mail: mnoorman@uitm.edu.my

protected and safeguarded from any forms of threats. According to Lopes and Sa-Soares (2012), in order to protect information "an organization implements a set of measures, also known as security controls, countermeasures, or safeguards, which can take many forms, such as policies, procedures, guidelines, practices, and organizational structure". Out of these various forms of controls, information security policy (ISP) is known to be the most popular approach advocated by the literature.

Nieles, Dempsey, and Pillitteri (2017), defined ISP as "an aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information". It has been claimed that an effective implementation or enforcement of ISP will help protect and safeguard organizational information assets from security threats (Jourdan, Rainer, Marshall, & Ford, 2010; Kimwele Mwangi, & Kimani, 2010; Lopes & Sa-Soares, 2012). However, the literature provides very limited empirical evidence to support this claim. The few available evidences were done involving small and medium enterprises (SMEs) or private companies. Not many evidences are available in the context of public agencies or organizations. According to Lopes and Sa-Soares (2012), the government or public administration should be the central focus of information security research because of the fact that they are the major investors in IT, plus the growing threats and challenges that they are facing.

Against this background, there is a need to examine ISP implementation and its relationship with security threats in the context of government setting. In particular, a study in the context of Malaysian government is deemed necessary because the government is one of the critical national information infrastructures (CNII) that needs to be protected and safeguarded (Cybersecurity Malaysia 2019). The disruption or destruction on the CNNI would have a devastating impact on national economic strength, national image, national defence and security and government capability to functions i.e. maintaining order to perform and deliver minimum essential public services (Cybersecurity Malaysia, 2019).

2. LITERATURE REVIEW

Diesch, Pfaff and Krcmar (2020) argued that, viewing information security as purely a technical concern and only assigning technical employees for information security responsibilities had proven ineffective. According to Peltier, Peltier and Blackley (2005), the first and probably most important aspect of information security is the security policy. The author further stressed that "if information security were a person, the security policy would be the central nervous system". The international standard of ISO/IEC (2005) for information security suggests that an ISP should contain (i) a definition of information security, its overall objectives, scope and the importance of security as an enabling mechanism for information sharing (ii) a statement of management intent, supporting the goals and principles of information security aligned with the business strategy and objectives (iii) a framework for setting control objectives (iv) a brief description of the security policies, principles, standards, and compliance requirements (v) definition of general and specific responsibilities for information security management (vi) references to documents which may support the policy, such as more detailed security policies and procedures for specific information systems or security rules users should comply with. Wu, Sun, and Wu (2020) argued that information security policies "provide rules for protecting an organization's information assets;

thus, the managers of all relevant communities must take policies as the basis for all information security plans, designs, and deployments".

Information security threats (IST) can be defined as "any potential danger to computers and network resources, like unauthorized access to confidential information, virus infection and system malfunction" (Bace, 2000). Information threats refers to obtaining specific information, and in most cases, it is confidential information of particular organizations and individuals. There are external threats caused by outsiders and internal threats normally caused by employees who are working in the organizations. Between external and internal, the later seems to be the most dangerous threats (Al-Mhiqani, Ahmad, Abidin, Yassin, Hassan, Abdulkareem, Ali, & Yunus, 2020). Al-Awadi and Renaud (2007) listed examples of internal threats as: abuse of computer access controls; damage by displeased employee; installation or use of unauthorized hardware, peripherals; physical theft of hardware or software; human mistake; use of organization resources for illegal communications or activities (porn surfing, email harassment) and installation or use of unauthorized software.

According to Chicherov and Norkina (2018) the key factors contributing to an increase in vulnerability of confidential data include (i) the massive amounts of information that is gathered, stored and processed using ICT (ii) single databases containing assorted information and varied ownership (iii) the increased number of potential users who have a direct access to database driven systems (iv) automation of machine-to-machine interaction and network information exchange. Sources of threats can come from both internal and external sources (Jouini, Rabai, & Aissa, 2014). The agents that caused security breaches are divided into three main classes, namely, human, environmental and technological. The objective of the attackers on a system can be either malicious or non-malicious while the intent of the human who caused the threat that can be intentional or accidental.

The impacts of the IST can be in the form of: (i) destruction of information, (ii) corruption of information, theft/ loss of information, (iii) disclosure of information, denial of use, (iv) elevation of privilege and (v) illegal usage. Ernst and Young (2018) classified the landscape of IST can be divided into three: common, advanced and emerging. The common category is the situation where attacks were carried out by novice by exploiting the known vulnerabilities using freely available hacking tools. The advanced category is for attacks that were normally executed by the experts by exploiting the complex and unknown vulnerabilities using sophisticated tools and methodologies. The emerging category is for attacks that executed by experts by focusing on vectors and vulnerabilities enabled by emerging technologies, identified through specific research

3. THEORETICAL FRAMEWORK

The Cybersecurity Strategic Headquarters (2016) stated that the fundamental principal of information security is "to ensure confidentiality, integrity, and availability of the information handled by government agencies according to the degree of importance of information, and it is a fundamental responsibility for each government agency to duly implement measures to ensure information security". In the context of Malaysian government, the Malaysian Administrative Modernization and Management Planning Unit or MAMPU has developed a handbook called MyMIS. MyMIS provides the standard guidelines which cover basic operation, technical operation

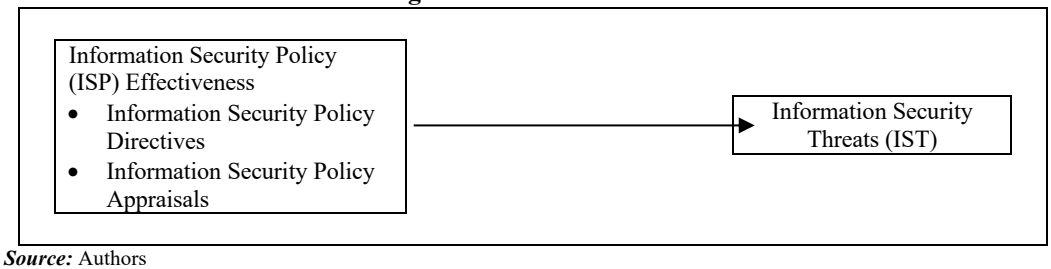
and legal matters on how to protect the government information assets especially for government sector (MAMPU, 2002). In addition, in 2016, MAMPU also launched Cyber Security Framework for Public Sector (RAKKSSA) which provides a high-level perspective of all necessary components of cyber security to be considered by the respective Government ministries and agencies to protect their information (data) in cyberspace. All government agencies are expected to enforce and implement both MyMIS and RAKKSSA.

As stated above, the literature provides few empirical evidences in relation to study examining the effectiveness of ISP. Adedayo and Ayobami (2013) studied the relationship between information security awareness and information security threat among university students. The results showed that community training; vulnerability to threat, perceived threat severity and compliance to security policies within the concept of information security awareness is positively related to IST. A study by Kimwele et al., (2010) involving Kenyan small and medium enterprises (SMEs) found that the majority had not adopted or implemented ISP and due to this, 76.2% of the participating SMEs had suffered some form of IST in the last 12 months. Recent study by Chinyemba amd Phiri (2018) found that Zambian public organizations are vulnerable to insider threats due to a number of factors that include; lack of security policies and procedures, technology complexity, financial gains, understaffing, lack of adoption and implementation of international security frameworks and standards such as ISO 27000 and COBIT.

Drawing upon the findings of abovementioned studies, this study developed a research model as shown in Figure 1. Based on the work of Martin and Da Veiga, (2015), the effectiveness of the ISP is measured in terms of ISP directives and ISP appraisal. ISP directive is defined as the clear direction or instruction on the protecting information security assets from information security incidents such as information security breaches that caused by unauthorized parties. ISP appraisals is defined as the evaluation of the information security policy, whether it is understandable, practical and successfully communicated. The literature suggests that when ISP of an organization is effective, the IST coming from internal or externals sources will be reduced. On the basis of this argument, the following hypothesis is put forward: *H1: There is a negative relationship between information security policy effectiveness and information security threats.*

The study developed hypothesis based on the main independent variable, termed as concept by Sekaran and Bougie (2010). In this study the independent variable has two dimensions. There are two options for developing the hypothesis, either based on concept or dimensions. If it is based on concept, also known as second order, it will be one hypothesis. But if it is based on dimensions, also known as first order, it will be two hypotheses. When the focus of the study is aimed at offering more generalizability, the second order approach is preferred as compared to first order (Arnau, 1998). Chen, Sousa and West (2005), explained that “second-order factor models can provide a more parsimonious and interpretable model when researchers hypothesize that higher order factors underlie their data”.

Figure 1: Research Model



Source: Authors

4. RESEARCH METHODOLOGY

The study used a survey research method with a questionnaire as the data collection instrument. The questionnaire was developed by the researcher. The first draft of the questionnaire comprised a total of 15 items, with the following breakdown: ISP directive (5 items), ISP appraisals (5 items), and IST (5 items). For each item, a Likert scale of five anchoring was used. As for the ISP directives and appraisals, the anchoring was between the two extremes of "1 = not practice at all" and "5 = highly practice". For the IST, the anchoring was between the two extremes of "1 = Never" and "5 = Always". The respondents were required to respond by ticking on these Likert scales. Before the actual data collection, several experts from the academic and industry were engaged to pre-test the questionnaires. Based on their comments and suggestions, the questionnaire was revised and refined accordingly. Following the pre-test exercise, a pilot test involving 30 respondents was performed. Their responses were analyzed and the results of the Cronbach alpha test indicated that all constructs scored values more than 0.7, suggesting that the questionnaire was reliable to be used in the study.

The unit of analysis of the study was firm or organization. The population of the study was Information Technology Department of agencies under the Malaysian Federal Ministries. At the time of data collection, there were 301 agencies under 25 ministries. Using a convenient sampling, a total of 295 questionnaires were distributed and 292 were returned and found useful for further analysis. This study used partial least square structural equation modelling (PLS-SEM) for analyzing the research data. The used of this approach for data analysis was considered appropriate because of its exploratory nature (Ramayah, Cheah, Chuah, Ting, & Memon, 2018).

SEM analysis involves two steps, the assessment of measurement model, also known as confirmatory factor analysis (CFA) and followed by the assessment of the structural model. The measurement model is assessed in terms of convergent validity and discriminant validity. The convergent validity is about the relatedness of the items in measuring the constructs while discriminant validity is concerned with the degree to which items differentiate across constructs. The hypothesized relationships amongst constructs are normally analyzed through structural model. The steps involve in assessing the structural model are (i) assessment of collinearity issues (ii) assessment of the significance and relevance of structural model relationship (iii) assessment of the coefficient of determination (R^2) (iv) assessment of effect size (f^2) and (v) assessment of predictive relevance (Q^2).

5. FINDINGS

5.1 Common Method Bias

Common method bias could be a major problem and a threat to the validity of the results. In a study that uses single source for collecting data, the problems of common method bias is always possible. Podsakoff and Organ (1986) stated that if one factor accounts more than 50% of the variance, the dataset is having the problem of common method bias. To this effect, the Harman's single factor test was performed. All items from all constructs were entered for analysis and constrained to a single factor. The results indicated that the single factor explained only 19.8% of the total variance, hence, suggesting that the collected data is free from the threats of common method variance.

5.2 Demographic Profiles

As the unit of analysis of the study was firm or organization, the IT manager was requested to represent the agency in responding to the questionnaire. In terms of gender, 167 or 57.2% were men while the rest were women (42.8%). In terms of age, the majority, aged between 36 and 40 (47.9%), followed by between 41 and 45 (39.1%) and between 31 and 35 (13.0%). In regards to length of service, 58.9% indicated to between 16 and 20 years, 38.7% between 11 and 15 years and 2.4% between 21 and 25 years.

5.3 Measurement Model

Table 1 presents the results of the convergent validity assessment of the measurement model. There were four items remained for measuring information security threats as one item had to be removed due to poor factor loading. In the same light, one item from information security policy directive and one information from security policy appraisal has to be eliminated due to factor loading less than 0.5. The criteria used for assessing convergent validity are factor loading, composite reliability (CR) and average variance extracted (AVE). The literature suggest that the factor loading should be above 0.700 but under certain circumstances values of 0.4, 0.5 and 0.6 are acceptable (Ramayah et al., 2018). The recommended values of CR and AVE are 0.7 and 0.5 respectively. The results as displayed in Table 1 suggest all of these criteria are fulfilled, hence, suggesting that convergent validity can be assumed.

Table 1: Assessment of Measurement Model

Constructs	Item Code	Item Statement	Factor Loading	Composite Reliability	Average Variance Extracted
Information Security Threats	OT_C11	Unauthorized outsiders pretended to be employees by phishing confidential information or data	0.824	0.845	0.577
	OT_C12	Unauthorized outsider blackmailed employees by installing ransomware to their computer	0.758		
	OT_C13	Unauthorized outsiders succeeded in spreading	0.738		

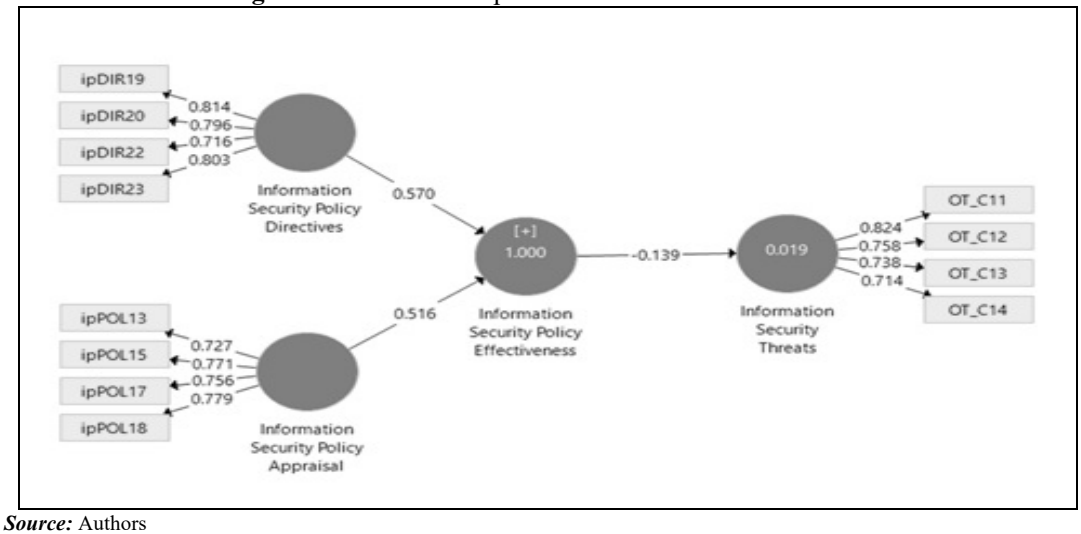
Constructs	Item Code	Item Statement	Factor Loading	Composite Reliability	Average Variance Extracted
		viruses and malware to employee's computer			
	OT_C14	Unauthorized outsiders succeeded in stealing organization's confidential data	0.714		
Information Security Policy Effectiveness	ipDIR19	Clear directives for the protection of stakeholder's information	0.785	0.844	0.575
	ipDIR20	Clear directives on the handling of information security incidents	0.742		
	ipDIR22	Clear directives on the prevention of information security breaches	0.624		
	ipDIR23	Clear directives for the compliance of organization's policy and procedures	0.747		
	ipPOL13	The Information security policy that is understandable by all employees irrespective of their ranks	0.649		
	ipPOL15	The information security policy that is well communicated to all employees irrespective of their ranks	0.666		
	ipPOL17	The information security policy that ensures regulatory compliance with various privacy and security laws	0.709		
	ipPOL18	The information security policy that regularly reviewed and updated	0.738		

Following the convergent validity assessment, the discriminant validity measure was performed using the Fornell and Larcker (1981). Discriminant validity can be assumed when the square root of the AVE of a construct is larger than the correlations between the construct and other constructs. The results as shown in Table 2 clearly suggest the criteria are fully met, implying that discriminant validity of the model can be assumed. The SmartPLS output of the measurement model is shown in Figure 2.

Table 2: Fornell and Larker (1981) Assessment of Discriminant Validity

	Information Security Threats	Information Security Effectiveness
Information Security Threats	0.760	-
Information Security Effectiveness	-0.139	0.709

Figure 2: SmartPLS Output of the Measurement Model



Source: Authors

5.4 Structural Model

Diamantopoulos and Siguaw (2006) explained that variance inflation factors (VIF) value of 3.3 or higher indicate potential collinearity problem. In this study, the highest VIF score for the inner model as 1.00, hence denoting that there was no issue of multicollinearity.

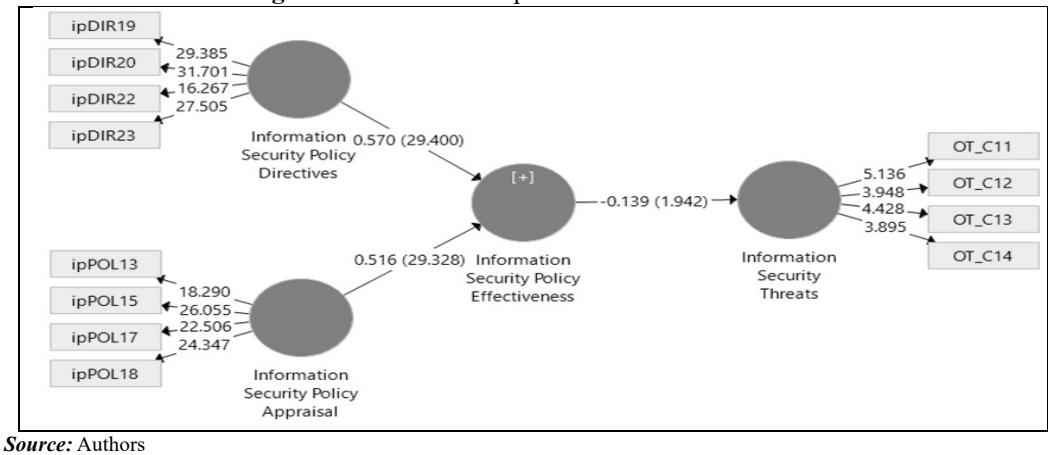
Table 3 presents the results of the hypothesis testing. The R^2 is 0.019, less than the recommended value of 0.10 by Falk and Miller (1992). However, the path between information security policy effectiveness and information security threats is still significant ($\beta = -0.139$, $p < 0.05$). According to Cohen (1988), f^2 value of 0.35, 0.15 and 0.02 are considered large, medium and small effect sizes respectively. In this study, $f^2 = 0.02$, which mean effect size is moderate.

As suggested by the literature, it is also important to examine the predictive relevance of the structural model, and this is done using the Stone-Geisser's Q^2 (Stone, 1974, Geisser, 1974). The results indicate that $Q^2 = 0.006$, which is well above zero, indicating that the model has predictive relevance. The SmartPLS output of the structural model is shown in Figure 3.

Table 3: Results of the Hypothesis Testing

	R^2	Std Beta	Std Error	T Value	P Value	f^2	Q^2
Information Security Policy Effectiveness → Information Security Threats	0.019	-0.139	0.066	1.942	0.018	0.02	0.006

Figure 3: SmartPLS Output of the Structural Model



Source: Authors

6. DISCUSSION

The objective of this study is to examine the relationship between ISP effectiveness and IST. A negative and significant relationship was hypothesized between the two constructs. The results of the analysis have clearly shown that the hypothesis was fully supported. This finding is almost consistent with that of Adedayo and Ayobami (2013); Kimwele et al., (2010) and Chinyemba and Phiri (2018).

As described in the preceding section, ISP effectiveness is operationalized as the combination of ISP directives and ISP appraisal. ISP directives relates to having a clear direction or instruction on the protecting information security assets from information security incidents. Both MyMIS and RAKKSSA developed by MAMPU are meant to be a general guideline. Government agencies are expected to develop their individual organisation ISP to govern and ensure that all activities carried out in their organisation adhere to the requirements stipulated in both documents. Hence, when developing the ISP, it has to clear so as to ensure that personnel at all levels of the government agencies understand their information security responsibilities to properly use and protect the information and resources entrusted to them.

ISP appraisal is concerned with the concerned with regular assessment and monitoring of the ISP. The is critical because "information security is not a static process and requires continuous monitoring and management to protect the confidentiality, integrity, and availability of information as well as to ensure that new vulnerabilities and evolving threats are quickly identified and

responded to accordingly" (Nieles et al., 2016). In the presence of a continuously evolving workforce and technological environment it is crucial that the government agencies provide timely and accurate information with regard to the ISP while operating at an acceptable level of risk.

The findings of the study have shown that, when ISP of an organization is found to be efficient and effective, the security threat posed to them will be minimized. As the number of employees working in the Malaysian federal government is huge, managing and controlling their behaviour in the workplace is not an easy task. Hence, the ISP should serve as a critical cornerstone in guiding employee behaviour to direct the protection of information. When the employees aware and understand the ISP requirements that they have to abide by, an information security-positive culture could be developed thereby reducing the amounts of security threats to the organization.

7. CONCLUSION

The contribution of the study can be described from two perspectives, namely, theoretical and managerial. From the theoretical perspective it has developed an empirical based framework connecting information security policy effectiveness and information security threats. The framework can be further tested in other setting by researchers who are interested in this topic. From the practical perspective, it sends a strong message to IS practitioners on the need to develop an effective information security policy.

Despite its contributions, this study has several limitations. Firstly, as shown in the result, the predictive power of information security policy is relatively small. The possible reason is that besides ISP, there are many other factors that can influence IST. Among them would be the establishment of information security culture (Masrek, Harun, & Sahid, 2018) and information technology capability (Alkabani, Deng, & Kam, 2014). Secondly, the time horizon of the data collection for this study was cross-sectional while the instrument used was perceptual measurement. Human perception by its nature changes over time. Hence, instead of collecting data at a single point in time, future researcher should consider adopting longitudinal study which will provide a better understanding of the relationships between variables.

ACKNOWLEDGEMENT

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

REFERENCES

Adedayo, W. S., & Ayobami, A. S. (2013). Relationship Between Information Security Awareness and Information Security Threat. *International Journal of Research in Commerce, IT & Management, 3*(8), 115-119.

Al-Awadi, M., & Renaud, K. (2007). Success Factors in Information Security Implementation in Organizations. In Kommers, P. (Eds.), *e-Society 2007: Proceedings of the IADIS International Conference e-Society* (pp. 169-176). Lisbon, Portugal.

Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Yassin, W., Hassan, A., Abdulkareem, K. H., Ali, N. S., & Yunos, Z. (2020). A Review of Insider Threats Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations. *Applied Sciences, 10,* 1-41.

Alkabani, A., Deng., H., & Kam, B. (2014, December 8-10). A Conceptual Framework of Information Security in Public Organizations for E-Government Development. In *Proceedings of the 25th Australiasian Conference on Information Systems* (pp. 179-189). Auckland, New Zealand.

Arnau, R. C. (1998, April 11). *Second-Order Factor Analysis: Methods and Interpretation*. Paper presented at the Annual Meeting of the Southwestern Psychological Association, New Orleans, USA.

Bace, R.G. (2000). *Intrusion Detection*. USA: MacMillan Publishing.

Chen, F. F., Sousa, K. H., & West, S. G. (2005). Testing Measurement Invariance of Second-Order Factor Models. *Structural Equation Modelling, 12*(3), 471–492.

Chicherov K. A., & Norkina A. N. (2018). Confidential Data Protection as a Means of Ensuring Information Security. *KnE Social Sciences, 3*(2), 85–88.

Chinyemba, M. K., & Phiri, J. (2018). An Investigation into Information Security Threats from Insiders and how to Mitigate them: A Case Study of Zambian Public Sector. *Journal of Computer Science, 14*(10), 1389-1400.

Cohen, J. (1988). *Statistical Power Analysis for The Behavioural Science*. Mahwah, New Jersey: Lawrence Erlbaum.

Cybersecurity Malaysia (2019). *About Critical National Information Infrastructure.* Retrieved from https://cnii.cybersecurity.my/main/about.html

Cybersecurity Strategic Headquarters (2016). *Common Standards for Information Security Measures for Government Agencies (FY2016*). Retrieved from https://www.nisc.go.jp/eng/pdf/Common%20Standards(FY2016).pdf

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative Versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration. *British Journal of Management, 17*(4), 263-282.

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A Comprehensive Model Information Security Factors for Decision Makers. *Computers & Security, 92,* 1-21.

Ernst & Young (2018). *2018 Top Cybersecurity Risk and Areas of Focus.* Retrieved from http://www.isaca.org/chapters1/puget-sound/education/Documents/2018%20Emerging%20Trends%20in%20Cybersecurity%20-%20EY%20ISACA%20Presentation%20-%2020MAR.pdf

Falk, R. F., & Miller, N. B. (1992), *A Primer for Soft Modelling* (1st ed). Ohio: University of Akron Press,

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, *Journal of Marketing Research, 19,* 39- 50.

Geisser, S. (1974). A Predictive Approach to the Random Effects Model, *Biometrika, 61*(1), 101-107.

ISO/IEC (2005). *ISO/IEC 27002 – Information Technology – Security Techniques – Information Security Management Systems – Requirements*. Retrieved from https://www.iso27001security.com/html/27002.html

Jouini, M., Rabai L. B. A., & Aissa, A. B. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science, 32,* 489 – 496.

Jourdan, Z., Rainer, R. K., Marshall, T. T., & Ford, F. N. (2010). An Investigation of Organizational Information Security Risk Analysis. *Journal of Service Science, 3*(2), 33-42.

Kimwele, M., Mwangi, W., & Kimani, S. (2010). Adoption of Information Technology Security Policies: Case Study of Kenyan Small And Medium Enterprises (SMES). *Journal of Theoretical and Applied Information Technology, 18*(2), 1-11.

Lopes, I. M., & Sá-Soares, Filipe de. (2012). Information Security Policies: A Content Analysis. (2012). In *Proceedings of the Pacific Asia Conference on Information Systems (PACIS) 2012*, Ho Chi Minh City, Vietnam.

MAMPU (2002). MyMIS - *Malaysian Public Sector Management of Information & Communication Technology Security Handbook*. Retrieved from https://jkrmlk.gov.my/1/dl.php?filename=Pengurusan%20Keselamatan%20ICT%20Sektor%20Awam%20Malaysia%20(MyMIS).PDF

Martins, N., & Da Veiga, A. (2015). An Information Security Culture Model Validated with Structural Equation Modelling. In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015),* Lesvos, Greece.

Masrek, M. N., Harun, Q. N., & Sahid, N. Z. (2018). Assessing the Information Security Culture in a Government Context: The Case of Developing Country. *International Journal of Civil Engineering and Technology, 9*(8), 96-112.

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2016). An Introduction to Information Security. National Institute of Standards and Technology. Retrieved from https://doi.org/10.6028/NIST.SP.800-12r1

Peltier, T. R., Peltier, J., & Blackley, J. (2005). *Information Security Fundamentals*. Boca Raton, Florida: Aeurbach Publication.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational Research: Problems and Prospects, *Journal of Management, 12*(4), 531-44.

Ramayah, T., Cheah, J., Chuah, F., Ting, H., & Memon, M. A. (2018). *Partial Least Squares Structural Equation Modelling (PLS-SEM) Using SmartPLS3.0: An Updated and Practical Guide to Statistical Analysis* (2nd ed). Kuala Lumpur, Pearson.

Sekaran, U., & Bougie, R. (2010). *Research Methods for Business: A Skill Building Approach*, (5th ed.) West Sussex, UK, John Wiley & Sons.

Stone, M. (1974). Cross-Validatory Choice and Assessment of Statistical Predictions, *Journal of the Royal Statistical Society, 36*(2), 111-147.

Wu, Y. C., Sun, R., & Wu, Y. J. (2020). Smart City Development in Taiwan: From the Perspective of the Information Security Policy. *Sustainability, 12,* 1-18.