THE ROLE OF TOP MANAGEMENT IN INFORMATION SECURITY PRACTICES

Mohamad Noorman Masrek[1]*, Qamarul Nazrin Harun[2], Ishak Ramli[3], Helmy Prasetyo[4]

[1]Faculty of Information Management, Universiti Teknologi MARA Selangor Branch, MALAYSIA, mnoormanm@gmail.com
[2]Faculty of Information Management, Universiti Teknologi MARA Selangor Branch, MALAYSIA, qamarulnaz@gmail.com
[3]Faculty of Arts and Design, Universiti Teknologi MARA, Perak Branch, MALAYSIA, ibr_86@yahoo.com
[4]Faculty of Social Sciences and Political Sciences, Universitas Airlangga, Surabaya, INDONESIA, helmy.prasetyo@fisip.unair.ac.id
*Corresponding Author

Abstract

A good number of literatures have indicated the importance of top management in ensuring the success of information security implementation. However, empirical research in the context of government agencies is still very scarce. In addition, in the context of Malaysia, little is really known on the situation of management supports in terms of information security practices. Against this background a study was conducted with the aim of examining the influence of top management support on information security practices. The top management support is operationalised as comprising of two dimensions, which are information security commitment and information security importance. Information security practices are operationalised as consisting of three dimensions namely, security policy effectiveness, information security responsibility, information security directives. The study hypothesised that the dimensions of top management support are significant predictors of the dimensions of information security practices. The survey research methodology and a convenient sampling was used in this study. The population was public organizations of Malaysian federal ministries. Based on 292 responses, a Partial Least Square Structural Equation Modelling (PLS-SEM) analysis was performed using SmartPLS Version 3.0 software. The results showed that the measurement model fulfilled all requirements for convergent validity and discriminant validity. The results of the structural model revealed that all exogenous constructs are significant predictors, implying that the hypotheses of the study are all accepted. The findings further highlight the need and importance of management support in ensuring the success of information security implementation. The contribution of the study can be gauged from several perspectives. From the theoretical perspective, it has developed an empirical based framework connecting top management support and information security practices. From the practical perspective, it has develop an instrument which can be used to self-evaluate the performance of organization information security practices.

Keywords: information security commitment, information security importance, information security policy effectiveness, information security responsibility, information security directives

1 INTRODUCTION

In this time and age, information is the most critical asset to many organizations. *Information* guides every decision an *organization* makes or expects to make. Thus, without the right, timely and

complete *information*, *organizations* are bound to make mistakes in making decisions. Due to that, the need to have information security is inevitable to any organizations. Through information security, organizational information can be protected from any threats or attacks.

Information security is defined as "the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (Nieles et al., 2017). The implementation of information security in organizations can be difficult when organizations do not get any support from the top management regarding the information security, or the top management do not understand the need or importance of an information security policy.

A good number of literatures have indicated the importance of top management in ensuring the success of information security implementation (Hsu & Wang, 2014; Nieles et al. 2017). However, empirical research in the context of government agencies is still very scarce. Lopes & Sa-Soares (2012) stated that research on information security should focus on the government instead or private companies because of the huge amount of IT investment that the government has spent. In addition, the government is the biggest creator and keeper of critical information of which any security breaches will results in the government not being able to perform their functions i.e. providing services to businesses and citizens. In the context of Malaysian government, little is really known on the situation of management supports in terms of information security practices. To this effect, a study was conducted with the aim of identifying the relationship between top management support and information security practices in agencies under Malaysian federal government.

The remainder of the paper is organized as follows. In the next section, we present the literature review and the research model with the corresponding hypotheses. In Section 3, we describe the research methodology of the study. We continue with discussion of empirical findings in Section 4. In Section 5 and 6, we conclude with discussion of the contributions and implications of our research.

2 LITERATURE REVIEW AND THEORETICAL FRAMEWORK

The essence of any information security practices is to ensure that the confidentiality, integrity and availability of information is maintained and preserved. Nieles et al. (2017) describe confidentiality as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information" while integrity as "guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity". Availability is concerned with ensuring timely and reliable access to and use of information.

In the context of Malaysian government, the Malaysian Administrative Modernization and Management Planning Unit or MAMPU has developed two information security guidelines, which are MyMIS and Cyber Security Framework for Public Sector (RAKKSSA). 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 while RAKKSSA 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. With MyMIS and RAKKSSA, the Malaysian public sector ministries and agencies shall develop their individual organisation information policy to govern and ensure that all activities carried out in their organisation adhere to the requirements stipulated in both documents. Hence, the role of the top management is crucial in making sure that information security policy is developed and enforced in their agencies or organizations.

According Hsu & Wang (2014), the research on information security shows that an information security program requires top management to be involved in, and take responsibility for, defining the parameters of risk management to preserve organizational assets. The ISO/IEC 17799 standard (2005) for information security clearly stated that commitment of senior management is critical for the implementation of information security measures. The top management commitment will normally translate into providing the moral and financial support for information security implementation. Thus, without top management's commitment and supports, the implementation of an information security measures will definitely fail.

Kankanhalli et al. (2003) examined the role of top management through a survey of IS managers from various sectors of the economy. The results showed that organizations with stronger top management support were found to engage in more preventive efforts than organizations with weaker support from higher management. Kazemi et al. (2012) conducted a survey of information security practices in Iranian Municipal Organizations. The results also showed that top management support was important in ensuring information security implementation. Alkabani, Deng & Kam (2014) explored three specific dimensions of information security culture, namely management commitments, accountability and information security awareness. The result suggested that management commitments, accountability, information security awareness, and social

pressure have a significant positive impact on information security compliance in public organizations

Sonnenschein et al. (2017) conducted a structured literature review to identify and organize factors that have been found to determine managerial IT security awareness. They found that the awareness of both top managers and managers at the department level is crucial for effective IT security management. Humaidi & Balakrishnan (2017) surveyed 454 healthcare professionals in three hospitals in Malaysia with the aim of examining the indirect effects of management support (MS) on user compliance behaviour (UCB) towards information security policies (ISPs). The results showed that top management support combined with other constructs from the Theory of Planned Behaviour were significant predictors of user compliance behaviour (UCB) towards information security policies (ISPs).

Drawing upon the findings discussed above, the study developed the research model as depicted in Figure 1. The independent variable is top management and consists of two dimensions which are information security commitment and information security importance. These dimensions are derived based on the work of Martin & Da Veiga (2015). The dependent variable is information security practises and comprised of three dimensions, namely, information security policy effectiveness, information security responsibility and information security directives. The operational definitions for the variables and the research hypotheses are shown in Table 1. All of the definitions are based on the work of Masrek et al. (2018).

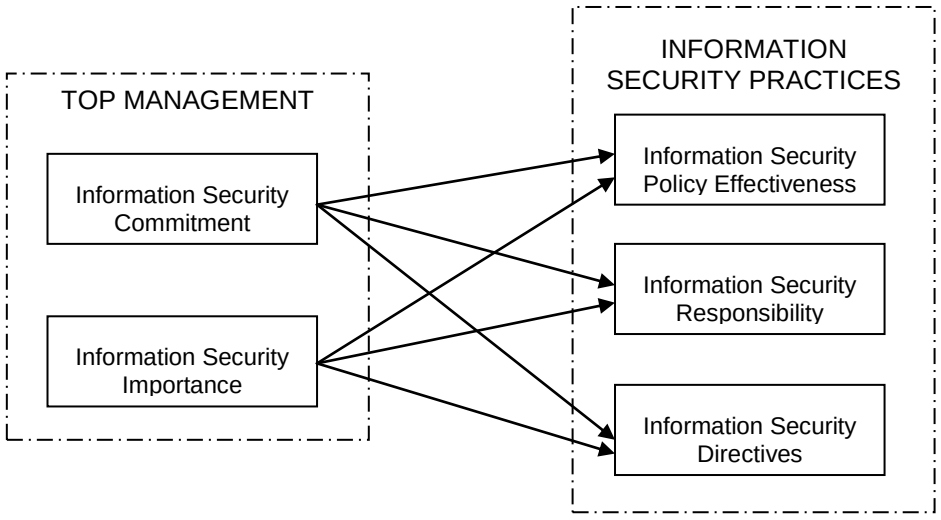

Figure 1: Theoretical Framework

Table 1: Constructs, Operational Definition & Hypothesis

Construct	Operational Definition	Hypothesis
Information Security Commitment	The degree to which top management give full supports and show their involvement towards an organizational initiative on information security.	Not applicable
Information Security Importance	The degree to which top management give preferences to information security as compared to any other activities	Not applicable
Information Security Policy Effectivess	The appraisal of the information security policy, whether it is understandable, practical and successfully communicated	H1: Information Security Commitment is a significant predictor of Information Security Policy Effectiveness H2: Information Security Importance is a significant predictor of Information Security Policy Effectiveness
Information Security Directives	The clear direction or instruction on the protection of information security assets from information security incidents such as information security breaches that caused by unauthorized parties.	H3: Information Security Commitment is a significant predictor of Information Security Directives H4: Information Security Importance is a significant predictor of Information Security Directives

Information Security Responsibility	The person or department responsible for ensuring the compliance of information security policies.	H5: Information Security Commitment is a significant predictor of Information Security Responsibility H6: Information Security Importance is a significant predictor of Information Security Responsibility

3 RESEARCH METHODOLOGY

Based on the guidelines provided by Noordin & Masrek (2016), the study adopted survey research methodology. A paper-based questionnaire was used for collecting the data. The items used in the questionnaire were mainly developed by the researcher. The first draft of the questionnaire comprised a total of 20 items. Each construct uses four items. For each item, a Likert scale of five anchoring was used. The anchoring used for each item was between the two extremes of "1 = not practice at all" and "5 = highly practice". Hence, the respondents were required to indicate the extent to which the listed items are being practiced in their organizations.

Prior to the main data collection, the questionnaire was pre-tested and pilot tested with several experts who were academicians and industry practitioners. Comments and suggestions given by them were used to revise the questionnaire. After the pre-test exercise, a pilot test was performed. 30 IT executives working with the agencies in the Malaysian federal government were engaged for the exercise. Their responses were analyzed to determine the reliability score of each construct based on Cronbach's Alpha. The results showed that the scores for all constructs were well above 0.7, implying that the questionnaire was reliable to be used in the study.

Given that the unit of analysis of the study was firm or organization, the population must be a list of agencies or organizations. In line with the purpose of the study, Information Technology Department of agencies under the Malaysian Federal Ministries was selected as the population of the study. Using a convenient sampling, a total of 295 questionnaires sent out to the IT managers of these agencies. These IT managers were requested to represent the agency in responding to the questionnaire. At the end of the data collection period 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, which involves two-stages analysis, namely, the assessment of measurement model and the assessment of the structural model. The measurement model is assessed in terms of validity and reliability of the research instrument while the structural model assesses the hypothesize relationship between constructs.

4 FINDINGS

The findings of the study are segmented into four sections, namely common method bias, demographic profiles, confirmatory factor analysis (CFA) or measurement model and structural model.

4.1 Common Method Bias

In a study that uses single data source, common method bias could be a serious threat that could jeopardize the validity of the results (Podsakoff & Organ 1986). Hence, to ascertain whether such threat is present in the dataset, the Harman's single factor test was executed. All items from all constructs were entered for analysis and constrained to a single factor. The results showed that the single factor explained only 22.3% of the total variance, less than the cut-off value of not more than 50%. Given this results, it can be safely assumed that that the collected data is free from the threats of common method bias.

4.2 Demographic Profiles

The profiles of these IT managers are shown in Table 1. In terms of gender, 167 or 57.2% were men while the rest were women (42.8%). In terms of age, the majority indicated to be aged between 36 and 40 (47.9%), followed by between 41 and 45 (39.1%) and between 31 and 35 (13.0%). As for the length of service, 58.9% indicated to have worked between 16 and 20 years, 38.7% between 11 and 15 years and 2.4% between 21 and 25 years.

4.3 Measurement Model

Table 2 presents the results of the convergent validity assessment of the measurement model. 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 is at least 0.7 and while for AVE is at least 0.5. The results as displayed in Table 2 suggest all of these criteria are met, suggesting that convergent validity can be assumed.

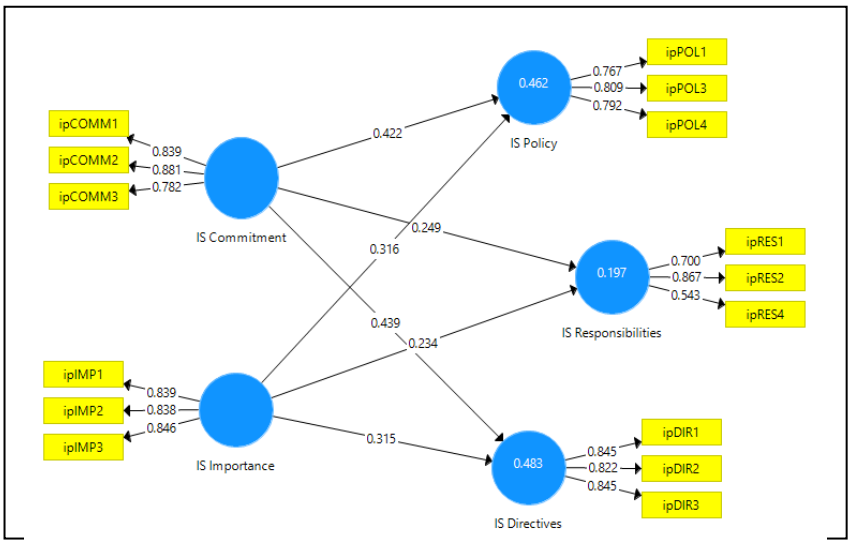

Figure 2: SmartPLS Output of the Measurement Model

Table 2: Assessment of Convergent Validity

Construct	Items	Factor Loadings	Composite Reliability (CR)	Average Variance Extracted
IS Commitment	ipCOMM1	0.839	0.873	0.697
	ipCOMM2	0.881		
	ipCOMM3	0.782		
IS Directives	ipDIR1	0.845	0.876	0.701
	ipDIR2	0.822		
	ipDIR3	0.845		
IS Importance	ipIMP1	0.839	0.879	0.708
	ipIMP2	0.838		
	ipIMP3	0.846		
IS Policy Effectiveness	ipPOL1	0.767	0.832	0.623
	ipPOL3	0.809		
	ipPOL4	0.792		
IS Responsibilities	ipRES1	0.700	0.753	0.512
	ipRES2	0.867		
	ipRES4	0.543		

Legend: IS = Information Security

Table 3 depicts the results of the discriminant validity assessment based on Fornell & Larker (1981) criteria. Discriminant validity can be assumed when the square root of the AVE is larger than the correlation value between constructs. The requirement is well fulfilled as the bolded and italicized values which represent the square root of the AVE are greater than the correlation values.

Table 3: Discriminant Validity Assessment Based on Fornell & Larker (1981)

	IS Commitment	IS Directives	IS Importance	IS Policy Effectiveness	IS Responsibilities

IS Commitment	***0.835***				
IS Directives	0.657	***0.837***			
IS Importance	0.690	0.618	***0.841***		
IS Policy Effectiveness	0.640	0.636	0.607	***0.789***	
IS Responsibilities	0.411	0.466	0.406	0.345	***0.716***

Legend: IS = Information Security

4.4 Structural Model / Hypothesis Testing

As to ascertain whether the inner model is free from the problem of muticollinerity, the VIF score are assessed. Diamantopoulos & Siguaw (2006) stated that variance inflation factors (VIF) value of 3.3 or higher indicate potential collinearity problem. The results indicated that none of the VIF scores surpassed 3.0 or 5.0 implying that issue of multinollinearity is not present in the data.

Table 4 presents the results of the hypothesis testing. All the paths between independent variables and dependent variables were significant with the t-values ranged between 2.794 and 6.688 ($p < 0.001$). The R^2 scores for the relationship between independent variables and dependent variables between 0.197 and 0.483, surpassed the recommended value of 0.10 by Falk & Miller (1992). Cohen (1988) noted that f^2 value of 0.35, 0.15 and 0.02 are considered large, medium and small effect sizes respectively. In this study, the f^2 for all paths are either small or 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 and Geisser's Q^2. The results indicate that the scores of Q^2 for all dependent variables are well above zero, implying that the model has predictive relevance. The SmartPLS output of the structural model is shown in Figure 3.

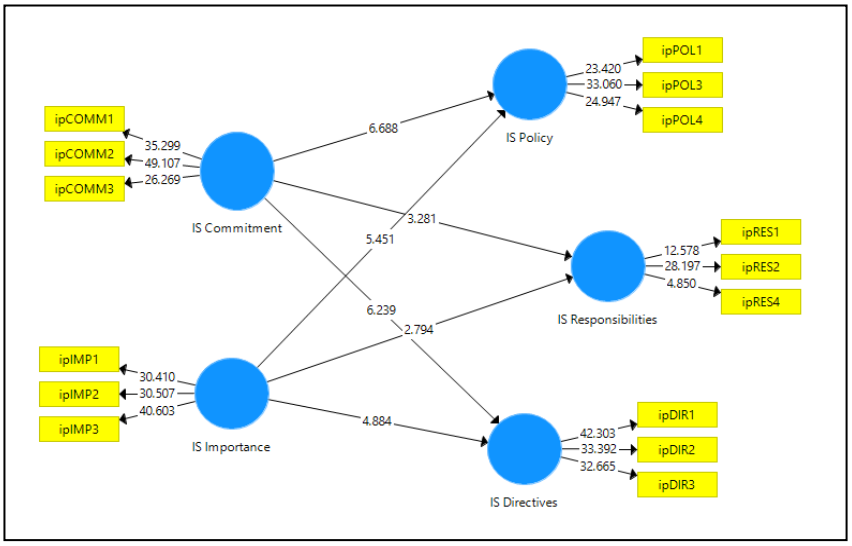

Figure 3: SmartPLS Output of the Structural Model

Table 4: Path Coefficient & Results of Hypothesis Testing

	R^2	Std Beta	Std Error	T Value	P Value	f^2	Q^2	Decision
H1: IS Commitment → IS Policy Effectiveness	0.462	0.422	0.063	6.688	0	0.174	0.270	Accept H1
H2: IS Importance → IS Policy Effectiveness		0.316	0.058	5.451	0	0.097		Accept H2

H3: IS Commitment → IS Responsibilities	0.197	0.249	0.076	3.281	0.001	0.041	0.081	Accept H3
H4: IS Importance → IS Responsibilities		0.234	0.084	2.794	0.005	0.036		Accept H4
H5: IS Commitment → IS Directives	0.483	0.439	0.07	6.239	0	0.196	0.316	Accept H5
H6: IS Importance → IS Directives		0.315	0.065	4.884	0	0.101		Accept H6

Legend: IS = Information Security

5 DISCUSSION

The objective of this study is to examine the relationship between top management and information security practices. Drawing upon this objective, six hypotheses are established. The results of the analysis clearly shown that all of the hypotheses are fully supported. This findings are almost in line with that of Kankanhalli et al. (2003), Kazemi et al. (2012), Alkabani, Deng & Kam (2014) and Humaidi & Balakrishnan (2017).

The findings of the study have shown that, when top management of an organization is found to be supportive and committed, information security practices will be effective. As the cases of security breach involving government agencies steadily increasing year by year, the need to have an effective information security practices is intensified. Information security breach or threats can come from internal or external sources. Internal threats occur when someone has authorized access to the information in the government agencies, for instance, access to network through legitimate account. External threats can arise from individuals or organizations working outside of the government agencies. They do not have authorized access to the information or network systems of the agencies. Between the internal and external threats, the former seems to be more challenging. Top management that is sensitive to the need of information security will develop and enforce information security policy, which lead to the development of positive information security culture. It is only thorough such culture, security threats or attacked can be overcome or mitigated.

As pointed out by Nieles et al (2017), "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". The regular assessment and monitoring of the information security practices is critical because attackers are extremely creative that they will always come up with new ways of stealing information or penetrating the network systems. It is only through proactive top management that this regular updating and assessment of information security practices can be materialized.

6 CONCLUSION

The contribution of the study can be viewed from two angles, which theoretical and managerial. From the theoretical view, it has developed an empirical based framework connecting top management role and information security practices. The framework can be further tested in other setting by researchers who are interested in this topic. From the practical view, it sends a strong message to IS practitioners on the need to have a strong support by the top management so as to ensure the success of the information security implementation in the organization.

While the study has achieved its objectives, it also has several limitations. Firstly, top management support is operationalized as comprising two dimensions only. Secondly, information security practice is operationalized as having three dimensions only. Future study can extend the framework by adding more dimensions to these variables. The third limitation of the study is associated with the time horizon of the data collection which is cross sectional. Collecting data at a single point in time may not be as accurate as collecting longitudinal data which will provide richer and deeper descriptions of situations.

7 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.

REFERENCE LIST

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

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

Diamantopoulos, A. and 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.

Falk, R.F. and Miller, N.B. (1992), *A Primer for Soft Modelling*, University of Akron Press, Akron, OH.

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

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

Hsu, C. and Wang, T., (2014). Composition of the Top Management Team and Information Security Breaches. In Maria Manuela CruzCunha (Ed.), Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance, Pennsylvania: IGI Global.

Humaidi, N. and Balakrishnan, V. (2017). Indirect Effect of Management Support on Users' Compliance Behaviour Towards Information Security Policies. *Health Information Management Journal*, 47(1), 17-27.

ISO/IEC 17799:2005. "Information Technology Security Techniques - Code of Practice for Information Security Management", ISO, Geneve.

Kankanhalli, A., Teo, H.H., Tan, B.C.Y. and Wei. K.K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), 139-154.

Kazemi, M., Khajouei, H., and Nasrabadi, H. (2012). Evaluation of Information Security Management Systems Success Factors: Case of Municipal Organization. *African Journal of Business Management*, 6(4), 4982-4989.

Lopes, I.M. and Sá-Soares, Filipe de, (2012). Information Security Policies: A Content Analysis. (2012). PACIS 2012 Proceedings. Paper 146. Available at: http://aisel.aisnet.org/pacis2012/146 (Retrieved 12 July 2018).

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

Noordin, S.A. & Masrek, M.N. (2016). Adopting the Quantitative and Qualitative Methods in the Social Science Research: Justifying the Underpinning Philosophical Orientation. *Proceeding of the 28th IBIMA Conference, 9-10 November 2016, Sevellie, Spain.*

Podsakoff, P.M. and 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., and 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.

Sonnenschein, R., Loske, A. and Buxmann, P. (2017). The Role of Top Managers' IT Security Awareness in Organizational IT Security Management. Proceedings of the 2017 International Conference on Information Systems (ICIS2017).