UNIVERSITI PUTRA MALAYSIA

INFORMATION SECURITY POLICY COMPLIANCE MODEL FOR GOVERNMENT AGENCY

MUHAMAD AMIRNAZMI BIN RAMLI

FSKTM 2018 50

INFORMATION SECURITY POLICY COMPLIANCE MODEL FOR GOVERNMENT AGENCY

MUHAMAD AMIRNAZMI BIN RAMLI

MASTER OF INFORMATION SECURITY

UNIVERSITI PUTRA MALAYSIA

2018

MUHAMAD AMIRNAZMI BIN RAMLI MASTER OF INFORMATION SECURITY 2018

INFORMATION SECURITY POLICY COMPLIANCE MODEL FOR GOVERNMENT AGENCY

By

MUHAMAD AMIRNAZMI BIN RAMLI

Thesis submitted to the School of Graduate Studies,
Universiti Putra Malaysia,
in Fulfilment of the Requirements for the Master of Information Security

JUNE 2018

DEDICATIONS

To my parents, project supervisor, lecturers, friends and internet. Thank you for making this possible.

ABSTRACT

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Information Security

INFORMATION SECURITY POLICY COMPLIANCE MODEL FOR GOVERNMENT AGENCY

By

MUHAMAD AMIRNAZMI BIN RAMLI

June 2018

Chair: **Dr. Azizol bin Haji Abdullah**

Faculty: **Faculty of Computer Science and Information Technology**

Abstract:

Aspects of information security is not sufficient to ensure a high level of information security policies of the organization are met. Behavior of non-

compliance with an organization's information security policy is not perfect if they are unable to establish the proper conduct of compliance with existing policies. Human attitude and behavior are the major contributing factors in every information security incident. Therefore, factors affecting their intentions on compliance behavior need to be identified. The purpose of this study is to identify the factors that use the most commonly used modeling elements in the field of psychology and social technology on information security. These factors will form the proposed model that will be validated with the results of a survey from the Information Management Division staff consisting of administrative staff and information technology officers. This study uses a quantitative approach because the most commonly used model design is used in the same field. Statistical software will also be used for analysis purposes in determining the frequency, reliability, and correlation of each factor against compliance in information security policy. A total of 142 respondents gave feedback and showed positive results on 11 factors which is 'Perceived Severity', 'Perceived Vulnerability', 'Response Efficacy', 'Self-Efficacy', 'Perceived Usefulness', 'Perceived Ease of Use', 'Attitude' 'Subjective Norms', 'Awareness', 'Reward' and 'Punishment'. Only one factor gives a negative response to 'Maladaptive Rewards'. The findings of this study will support the proposed compliance model and will guide each government agency in solving the problem of employee behavior in turn will affect the safety of organizational information.

ABSTRAK

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Sarjana Keselamatan Maklumat

MODEL PEMATUHAN TERHADAP POLISI KESELAMATAN MAKLUMAT UNTUK AGENSI KERAJAAN

Oleh

MUHAMAD AMIRNAZMI BIN RAMLI

Jun 2018

Penyelia: **Dr. Azizol bin Haji Abdullah**

Fakulti: **Fakulti Sains Komputer dan Teknologi Maklumat**

Abstrak:

Aspek keselamatan maklumat tidak mencukupi untuk memastikan tahap bagi dasar keselamatan maklumat dalam organisasi itu dipatuhi. Tingkah laku bagi ketidakpatuhan pekerja terhadap dasar keselamatan maklumat

sesebuah organisasi itu adalah tidak sempurna jika mereka tidak dapat membentuk sikap yang betul bagi melaksanakan pematuhan dasar sedia ada. Sikap dan tingkah laku manusia merupakan faktor penyumbang utama dalam setiap insiden keselamatan maklumat. Oleh itu, faktor yang mempengaruhi niat mereka terhadap tingkah laku pematuhan perlu dikenal pasti. Tujuan kajian ini adalah untuk mengenal pasti faktor-faktor yang menggunakan unsur pemodelan yang biasa digunakan dalam bidang psikologi dan teknologi sosial terhadap keselamatan maklumat. Faktor-faktor ini akan membentuk cadangan model yang akan disahkan dengan hasil tinjauan kaji selidik dari kakitangan Bahagian Pengurusan Maklumat yang terdiri daripada kakitangan pentadbiran dan pegawai teknologi maklumat. Kajian ini menggunakan pendekatan kuantitatif kerana reka bentuk model yang paling biasa digunakan dalam bidang yang sama. Perisian statistik juga akan digunakan untuk tujuan analisis dalam menentukan kekerapan, kebolehpercayaan, dan korelasi setiap faktor terhadap pematuhan dalam dasar keselamatan maklumat. Seramai 142 responden telah memberikan maklum balas dan menunjukkan keputusan positif terhadap 11 faktor iaitu 'Persepsi Kelemahan', 'Persepsi Impak', 'Keberkesanan Tindakbalas', 'Keupayaan Diri', 'Persepsi Kebergunaan', 'Persepsi Mudah Digunakan', 'Sikap', 'Norma Subjektif', 'Kesedaran', 'Ganjaran' dan 'Hukuman'. Hanya 1 faktor sahaja yang memberikan tindak balas negatif iaitu 'Ganjaran Ketidakpatuhan'. Hasil kajian ini akan menyokong model pematuhan yang dicadangkan dan akan menjadi panduan dalam setiap agensi kerajaan dalam

menyelesaikan masalah tingkah laku pekerja seterusnya akan memberi kesan kepada keselamatan maklumat organisasi.

ACKNOWLEDGEMENTS

First of all, I would like to thank my parents for their support in my journey to complete my year as a Master student. Especially, I would like to express my appreciation to my supervisor, Dr. Azizol bin Haji Abdullah who has guided and assisted me in completing the Master's project in sharing knowledge, experience, advice and teaching throughout the research period. Indeed your encouragement and expertise have also shaped me in this research work. I would also like to thank all the respondents of the government staff who served in the Information Management Division, Ministry of Defense in helping me to provide feedback on this survey. Without you, this research project is not implemented successfully. Thank you to all Universiti Putra Malaysia lecturers and students as well as my colleagues who are involved directly or indirectly in this research. It's a wonderful time to learn and share knowledge with many people throughout the research period. With their help, their opinions and expertise, all this has been done. Thanks to the virtual media, the internet and journals and related brochures for providing information even when it is easy to find. Finally, it is hoped that this project will be able to serve as a guide in generating risk assessment factors on existing policies in government agencies.

APPROVAL

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Information Security. The members of the Supervisory Committee were as follows:

DR. AZIZOL BIN HAJI ABDULLAH

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Supervisor)

Date: June 2018

DECLARATION

- Declaration by graduate student
- I hereby confirm that:
- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials asstated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012.

Signature: _____ Date: _____

Name and Matric No.: MUHAMAD AMIRNAZMI BIN RAMLI (GS46953)

TABLE OF CONTENTS

LIST OF TABLES

TABLE NO.

LIST OF FIGURE

FIGURE NO.

CHAPTER 1

INTRODUCTION

1.1 Background

Every government agency is required to implement Information and Communication Technology Security Policy (ICTSP) as recommended by the Malaysian Administrative Modernization and Management Planning Unit (MAMPU) in 2001. It is intended as an enhancement of information handling using ICT equipment. Among the key factors that created the policy were due to the importance of security for IT assets. This is because all the assets involved contain and store important government information. At the same time, it is to ensure that confidentiality, integrity and availability of data are maintained optimally[1]. As ICTSP differs and is housed in every government business function, they share the same goal of ensuring the continuity of the agency by minimizing the impact and probabilities of IT-related security incidents. Among the ICTSP goals implemented in the government IT department are the dissemination of information contained in the policy itself, a comprehensive policy consistent with current changes, protection of IT assets from any form of abuse or breach, ensuring business continuity by minimizing the impact of the incident and providing security awareness to customers which includes public servants of government agency as well as suppliers or contractors. As the IT department functions as a central point of

information management for government agency, it is an ideal choice for the scope of this study as it handles information systems with the use of ICT platforms that need to implement ICTSP, and procedures in their operations to ensure information security is guaranteed.

This study was conducted by focusing on Information Technology (IT) Department at a government agency, Information Management Division, Ministry of Defense located in Kuala Lumpur. The function of this IT department is to manage every service offered by government agency through the use of information systems including network infrastructure and hardware. The division comprises 160 employees, comprising the 'F' team of Information Technology. The minority consists of the 'N' group of the establishment of ICT governance. The division is headed by a director, the Division Secretary acting as Information and Communications Technology Security Officer (ICTSO). The agency has also been available to handle system management and network operations including the management of IT agency IT assets. There are several important systems administered by the Department including e-mail applications, human resource management applications, accounting applications, as well as related service applications by other departments[2]. This operated operation is to ensure that the system runs without interference and is intended as a protection against any form of internal and external threats. All of these systems are operated and controlled using network and security hardware such as routers, switches, web

application firewalls and the Infusion Prevention System (IPS). In the data center environment, any confidential information of this agency is stored in a physical server and can be categorized as "Mini-Cloud" accessible from the outside. All of these servers are protected by "Layer 7" hardware, Web Application Firewall (WAF), which can run cross-site scripts (XSS) and SQL injection [3].

1.2 Problem Statement

Information security policies contain procedures, standards and guidelines on how to ensure information security when using compliance with their operations. Human behavior must be considered and taken into account in maintaining information security as they need to understand the threats and protective measures that have been implied in the policies and procedures [4]. Most security incidents occur because of behavior that does not comply with employees on ICT policy or information security procedures [5]. Failure to comply with this will occur with security incidents involving cases such as leakage of information and computer abuse that will cause the organization to suffer financial loss in turn affecting the reputation of the organization [6]. It is therefore important to identify factors that contribute to employee compliance as it can assist information security officers in addressing issues related to their efforts in providing solutions to addressing employee behavioral issues [7].

On the basis of this topic, issues in the ICT Security Policy at government agency are behavioral compliance in employees. Factors affecting the compliance intent are important as it is an example of the actual behavior of an employee who can be a compliance or non-compliance with the policy. The purpose of this research is to identify the factors of the proposed model based on past studies on the model of information security policy compliance that can assist the public sector in minimizing risks and threats from employee behavior.

1.3 Research Questions

i. What are the factors that affect compliance with the ICT security policy information in the organization?

ii. How to design an information security compliance model for government agency?

iii. How to evaluate the proposed model?

1.4 Research Objective

i. To identify and propose factors that affect adherence to the organization's information security policy.

ii. To design the ICT information security compliance model in government agencies.

iii. To evaluate the compliance model for information security policies proposed at government agencies based on the frequency, reliability, and correlation of each factor.

1.5 Scope of Study

The scope of this study focuses on the Department / IT Division in a government agency comprising administrative officers and IT officers handling valuable information at agency that mostly use digitally managed and stored information systems. All staff are equipped with workstations (computers) and have access to both internal and external networks (intranets / internet) as part of their daily operating needs. Part of the survey will include a questionnaire that will be given directly to each employee as it is required to comply with the information security policy specified by the government agency.

1.6 Thesis Structure

The summary of thesis structure was shown below:

Chapter 1 – Briefly describes about introduction which is the background, problem statement, research questions, research objectives and scope of study

in conducting a research work on the Information Security Policy Compliance Model for Government Agency.

Chapter 2 – This chapter focused on extensive literature review from relevant publications to understand more about the variety of Information Security Model towards to compliance intension. This includes a number of theories to be considered for use in this project.

Chapter 3 – This section covers a full phase of methodology that will be using throughout this research design, data gathering method, data analysis, pilot survey, research procedure, operational framework, research planning and schedule also limitations. It also covers the technical requirements and specifications that will be needed in order to develop the algorithm for syntax to calculate all variable.

Chapter 4 – This section discusses the proposed model of compliance and also the hypothesis of the whole variable of the model used.

Chapter 5 – This section discusses the reading results of each model based on three objective requirements such as frequency, reliability test and correlation of each factor.

Chapter 6 - As the final chapter for the thesis, the summary of research works will be elaborated here.

1.7 Limitation

Some of the limitations in this study are as follows:

i. Factors towards information security policy compliance purposes may differ among respondents because it involves different scope of work of each respondent. It is also an individual assumption about the individual's response to the feedback received for the entire study.

ii. Target population conditions are small and may result in lack of data accuracy.

1.8 Summary

This section as a whole describes an overview of background studies and problems on existing security policies, problem statements and the type of research that they wish to implement. From the statement of the problem, goals and survey questions should be identified to achieve the stated objectives. In order to complement this research, the scope of the study should be determined to ensure that the results are produced according to the suitability of the environment. The benefits of this study will contribute to the overall goal of information security policy thus minimizing the rate of occurrence of information security incidents.

REFERENCES

[1] K. S. Negara, "PEKELILING AM BIL. 1 TAHUN 2001." 2001.

[2] L. P. U.-U. Malaysia, *AKTA AKTIVITI KERAJAAN ELEKTRONIK 2007*. 2007.

[3] A. Razzaq, A. Hur, S. Shahbaz, M. Masood, and H. F. Ahmad, "Critical analysis on web application firewall solutions," *Auton. Decentralized Syst. (ISADS), 2013 IEEE Elev. Int. Symp.*, pp. 1–6, 2013.

[4] S. Furnell and N. Clarke, "Power to the people? the evolving recognition of human aspects of security," *Comput. Secur.*, vol. 31, no. 8, pp. 983–988, 2012.

[5] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Inf. Manag.*, vol. 49, no. 3–4, pp. 190–198, 2012.

[6] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. Secur.*, vol. 56, pp. 1–13, 2016.

[7] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: an Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2010.

[8] I. Tipton, H. F., Krause, and Mick, *Information Security Management Handbook*, no. 5. 2004.

[9] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, "Employees' information security awareness and behavior: A literature review," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2013, pp. 2978–2987.

[10] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *J. Exp. Soc. Psychol.*, vol. 19, no. 5, pp. 469–479, 1983.

[11] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, 2012.

[12] P. Norman, H. Boer, and E. R. Seydel, "Protection motivation theory," *Predicting Health Behaviour: Research and Practice with Social Cognition Models*. pp. 81–126, 2005.

[13] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Q.*, vol. 13, no. 3, p. 319, 1989.

[14] J. Zhang, B. J. Reithel, and H. Li, "Impact of perceived technical protection on security behaviors," *Inf. Manag. Comput. Secur.*, vol. 17, no. 4, pp. 330–340, Oct. 2009.

[15] A. Turan, A. Ö. Tunç, and C. Zehir, "A Theoretical Model Proposal:

Personal Innovativeness and User Involvement as Antecedents of Unified Theory of Acceptance and Use of Technology," *Procedia -Social Behav. Sci.*, vol. 210, pp. 43–51, 2015.
[16] A. Al-Omari, O. El-Gayar, and A. Deokar, "Security policy compliance: User acceptance perspective," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 3317–3326, 2011.
[17] V. Venkatesh and Davis, "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Manage. Sci.*, vol. 46, no. 2, pp. 186–204, 2000.
[18] I. Ajzen, "The theory of planned behavior," *Orgnizational Behav. Hum. Decis. Process.*, vol. 50, pp. 179–211, 1991.
[19] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *Source MIS Q.*, vol. 27, no. 3, pp. 425–478, 2003.
[20] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," *Comput. Secur.*, vol. 53, pp. 65–78, 2015.
[21] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Comput. Secur.*, 2010.
[22] I. Ajzen, "Perceived behavioral control, self-efficacy, locus of control, and the Theory of Planned Behavior," *J Appl Soc Psychol*, vol. 32, no. July, pp. 665–683, 2002.
[23] A. Bandura, "Social cognitive theory of self-regulation," *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 248–287, 1991.
[24] P. A. Pavlou and M. Fygenson, "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," vol. 30, no. 1, pp. 115–143, 2006.
[25] D. Goodhue and D. Straub, "Security concerns of system users: a study of perceptions of the adequacy of security," *Inf. Manag.*, 1991.
[26] M. T. Siponen, "A conceptual foundation for organizational information security awareness," *Inf. Manag. Comput. Secur.*, vol. 8, no. 1, pp. 31–41, 2000.
[27] S. Boss, L. Kirsch, I. Angermeier, and R. Shingler, "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security," *Eur. J.*, 2009.
[28] S. R. Boss and L. J. Kirsch, "The last line of defense: Motivating employees to follow corporate security guidelines," *Icis*, pp. 1–18, 2007.
[29] D. Straub and R. Welke, "Coping with systems risk: security planning models for management decision making," *Mis Q.*, vol. 22, no. 4, pp. 441–469, 1998.
[30] P. M. Podsakoff, W. H. Bommer, N. P. Podsakoff, and S. B. MacKenzie, "Relationships between leader reward and punishment behavior and subordinate attitudes, perceptions, and behaviors: A meta-analytic review of existing and new research," *Organ. Behav. Hum. Decis.*

Process., vol. 99, no. 2, pp. 113–142, 2006.
[31] S. Landau and B. Everitt, *A handbook of statistical analyses using SPSS.*, vol. 24, no. 20. 2004.
[32] B. P. Rob Eisinga, Manfred te Grotenhuis, "The reliability of a two-item scale: Pearson, Cronbach or Spearman-Brown?," *Radboud Repos.*, p. 144, 2013.
[33] J. R. Draugalis and C. M. Plaza, "Best Practices for Survey Research Reports Revisited : Implications of Target Population , Probability Sampling , and Response Rate," vol. 73, no. 8, pp. 2–4, 2009.
[34] A. Barua, "Methods for Decision-Making in Survey Questionnaires Based on Likert Scale," *J. Asian Sci. Res.*, vol. 3, no. 1, pp. 35–38, 2013.
[35] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," *Comput. Secur.*, vol. 53, pp. 65–78, 2015.
[36] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of," *MIS Q.*, vol. 13, no. 3, p. 319–340., 1989.
[37] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2010.
[38] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297–334, 1951.
[39] M. Smith, *Statistical Analysis Handbook*. 2014.