INFORMATION SECURITY POLICY COMPLIANCE MODEL FOR PUBLIC SECTOR

FUAD HARRIZ BIN ABD RAHIM

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Science (Information Assurance)

Advanced Informatics School
Universiti Teknologi Malaysia

JUNE 2017

To my beloved family, supervisor and friends.

ACKNOWLEDGEMENT

First and foremost, I want to express my gratitude to ALLAH S.W.T The Most Gracious who give me strength and patience to undertake this project successfully. I am grateful to my family who gave their supports throughout my life and in my studies. I would also like to express deepest gratitude to my supervisor, Dr Ganthan Narayana Samy, for his numerous consultation, professional guidance, patience and support throughout my research. Without his supervision and constant help, this research would not have been possible. Finally, I would also like to thank my course mates and friends for their valuable advices and encouragement.

ABSTRACT

Technical aspect of security is inadequate to ensure information security within organization thus requires for adoption of information security policy. Policy without compliance from the employee of an organization would be useless where it requires desirable behaviours. Human are known to be the weakest link in information security thus factor that affect their intention towards compliance behaviour should be identified. The purpose of this research is to identify factors from recent researches that uses the most common compliance model used in social psychology and technological domain. These factors would then be built up into a proposed model where it will be validated with the survey questionnaire result from an IT department that consists of administrative and IT professionals. This research uses quantitative approach as it is the most used research design used in this domain and statistics software will be used to determine the frequencies, reliability, and the correlation of the factors towards compliance intention. According to 214 respondents, eleven factors have been concluded to have significant impact towards compliance intention that is perceived severity, perceived vulnerability, maladaptive rewards, response efficacy, self-efficacy, attitude, subjective norm, perceived usefulness, perceived ease of use, awareness and punishment while rewards have insignificant relation. The result from this research would support the proposed model that will act as a guidance in public sector to solve issues regarding employee behaviour that impacts information security policy compliance.

ABSTRAK

Aspek keselamatan teknikal sahaja adalah tidak mencukupi dalam memastikan keterjaminan maklumat dalam sesebuah organisasi maka memerlukan adaptasi polisi keselamatan maklumat. Polisi tanpa pematuhan daripada pekerja sesebuah organisasi akan menjadi sia-sia di mana ia memerlukan tingkah laku yang wajar. Tindakan manusia dikenalpasti sebagai penyebab utama dalam insiden keselamatan maklumat maka faktor yang memberi impak kepada niat mereka terhadap kelakuan pematuhan perlu dikenalpasti. Tujuan kajian ini adalah untuk mengenal pasti faktor-faktor dari penyeldikan terkini yang menerapkan model pematuhan yang paling kerap digunakan dalam bidang psikologi sosial dan penerimaan teknologi. Faktor-faktor ini kemudiannya akan membentuk cadangan model yang mana ianya akan disahkan dengan hasil kajian soal selidik dari jabatan teknologi maklumat yang terdiri daripada pekerja pentadbiran dan pegawai teknologi maklumat. Kajian ini menggunakan pendekatan kuantitatif kerana ia adalah reka bentuk yang paling kerap digunakan dalam bidang yang sama dan perisian statistik akan digunakan untuk tujuan analisis dalam menentukan kekerapan, kebolehpercayaan, dan korelasi setiap faktor terhadap niat pematuhan polisi keselamatan maklumat. Menurut 214 responden, terdapat sebelas faktor yang mempunyai pengaruh ke atas niat pematuhan iaitu persepsi impak, persepsi kelemahan, ganjaran ketidakpatuhan, keberkesanan tindakbalas, keupayaan diri, sikap, pengaruh persekitaran, persepsi kebergunaan, persepsi mudah digunakan, kesedaran dan hukuman manakala ganjaran tidak mempunyai impak positif. Hasil dari kajian ini akan menyokong model pematuhan yang dicadangkan yang akan bertindak sebagai panduan dalam sektor awam dalam menyelesaikan isu-isu kelakuan pekerja yang membawa impak terhadap pematuhan polisi keselamatan maklumat organisasi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

This research involves an Information Technology (IT) department within a Malaysian government agency located at Kuala Lumpur that have implemented an information security policy. The function of the IT department is to manage each service offered by the government agency through the use of information system including its infrastructure of networks and appliances. It is lead by a director that act as an Information and Communication Technology Security Officer (ICTSO) for the government agency and structured into two smaller branches that handles the management of the systems and the network operation including the IT assets management of the government agency. The systems managed by the IT department includes the use of email, human resources, accounting, and related services by other department within the government agency that requires the translation of business process into electronic form (Malaysia & Lembaga Penyelidikan Undang-Undang, 2009). The operation handled is to ensure that the system running without any disruption and for protection purpose from any form of insider and outsider threat which includes the implementation of appliances such as routers, switches, web application firewall and Intrusion Prevention System (IPS). This include the implementation of a data centre that holds the physical servers and appliances that is crucial for the whole infrastructure.

Each government agency is required to implement Information and Communication Technology Security Policy (ICTSP) as requested by the Malaysian Administrative Modernization and Management Planning Unit (MAMPU) back in the year 2000 with the rise of information handling using ICT appliances at that time. The main concern of the policy is the IT assets security of each government agency as it also includes the important information characteristics of confidentiality, integrity, availability, non repudiation and validity (MAMPU, 2000). As ICTSP is different and localized according to each government agencies business function, they share the same aim that is to ensure business continuity by minimize the impact and probability of IT related security incidents. According to security incident statistics by Malaysia Computer Emergency Response team (MyCERT), there are a total of 7698 cases as now have been reported by individual and various organizations related to information security for the year 2016 (MyCERT, 2016). Those cases includes incident such as fraud, spam and intrusion that involves human behaviour as the weakest link in aspects of information security within an organization (Metalidou *et al*., 2014) which can relate back to policies that must be adhered by every employees. Among the objectives of the ICTSP that is implemented on the IT department is dissemination of management stand point on the policy itself, comprehensive policy that is accordance with current changes, IT assets protection from any form of abuse or infringement, ensure business continuity by minimize the impact of incident and to provide security awareness to clients which include civil servants of the government agency and suppliers. Since the IT department act as a centre point of information management for the government agency, it is a viable choice for the scope of this study as it handles information system with the use of ICT platform that need to apply ICTSP and further standards, and procedures in their operation to ensure information security.

1.2 Background of the Problem

Most organization and companies nowadays have changed their traditional work environment to a more paperless information system with the rely and investment on IT appliances (Ifinedo, 2014). Although it provides better business management with benefits that would save operational costs and effective information handling, the

aspect of information security should not be disregard. Confidentiality, integrity, availability, non-repudiation and authorization were among the key elements of information that must be guarded to ensure security. As most organization would opt to strategize their environment security solely on using technological related IT hardware and software such as network firewall, Intrusion Detection System (IDS), Web Application Firewall (WAF), antivirus and authorization systems, it is found out that it is not enough to ensure security from incidents involving information of the organization (Sohrabi Safa *et al*., 2016; Safa *et al*., 2015). Hence, the focus of information security has shifted onto the organizational perspective and its employee on complying with the stated information security policy where employees are known to be the weakest link in an organizations information security (Warkentin & Willison, 2009).

Information security policy contains procedures, standards and guidelines on how to ensure information security when employing adhering to their operational work. The human behaviour must be taken into consideration in maintaining the security of information as they need to understand the threat and safeguard measures that have been implied within the policies and procedures (Furnell & Clarke, 2012). Most of security incidents happened because of incompliance behaviour of the employees towards the organization information security policies and procedures (Vance *et al*., 2012). These act of incompliance would end up with security incidents involves cases such as information leak and computer abuse that would causes the organization to suffer financial and also reputation loss (Sohrabi Safa *et al*., 2016; Herath & Rao, 2009). According to a survey done in the United States involving public sectors, health institutions and universities, nearly half or 44% of the incidents comes from insiders of the organization where it involves mostly with incidents of malware infections and network abuse (Richardson & Director, 2008; Chen *et al*., 2012). Therefore, it is important to identify factors that contribute to employees compliance intention as it may help information security managers in overcoming issues related to their effort as well as to provide solutions in solving behavioral issues of the employees (Bulgurcu *et al*., 2010).

1.3 Statement of the Problem

Based on the background problem, the issue in information security policy in organizations are similar to what the government agency experienced regarding compliance behaviour within employees. Government agencies which are part of the Critical National Information Infrastructure (CNII) sector plays a role to maintain valuable assets includings systems that are crucial to the nation where a threat towards information security may have impact on the nations influential image, sovereigity and capability to deliver services to the public (Yunos *et al*., 2010). Factors that affect the compliance intention are important as it is a precedent to actual behaviour of an employee that could be compliance or non-compliance towards the policy.

1.4 Aim of Research

The aim for this research is to identify factors that affects compliance intention from a proposed model based on recent studies that may aid the public sector in minimizing risk and threat from employees behaviour regarding the ICTSP.

1.5 Research Questions

The main questions in this research are as follows:

i. What are the factors that influence compliance towards information security policies in public sectors?
ii. How to design the information security policy compliance model for public sectors?
iii. How to evaluate the proposed model?

1.6 Research Objective

The objectives of this study are as below:

i. To identify the factors that influence compliance towards information security policies in public sectors
ii. To design an information security policy compliance model in public sectors
iii. To evaluate the proposed information security policy compliance model for public sectors

1.7 Scope of Study

The scope of this research in based on an IT department of a government agency that consists of administrative clerks and IT professionals that handles valuable information of the government agency mostly using information system that is managed and stored digitally. The employees are well equipped with workstations and having access to the internal network and internet as part of their daily operation requirement. Part of this research will include survey questionnaire that will be given directly to each parties of employee as they both are needed to comply with the stated information security policy of the government agency.

1.8 Significance of the Study

Theoretically, this research will present a compliance model that is based on validated factors towards information security policy compliance intention. It may also serve as a guidance for the IT management on each government agency in the public sector to better understand and solve behavioral issues of their employees related to information security. The result from this research may also contribute to strategy

planning of the organization to increase the value of identified factors that may significantly contribute towards compliance of the information security policy.

1.9 Thesis Outline

This chapter explains the overview of the study and provide background problem where statement of the issue then be stated. From the problem statement, the aim and research question were to be identified and research objectives will be the focus of this study within the predefined scope. The benefit of this study would contribute to the domain of information security.

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248.

Ahlan, A., Arshad, Y., & Lubis, M. (2011). Implication of human attitude factors toward information security awareness in Malaysia public university. *Proceedings in International*.

Ajzen, I. (1991). The Theory of Planned Behaviour. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Ajzen, I. (2002). Perceived Behavioral Control, Self Efficacy, Locus of Control and the Theory of Planned Behaviour. *Journal of Applied Social Psychology*, *32*(4), 665–683.

Ajzen, I. (2005). *Attitudes, personality, and behavior*. UK: McGraw-Hill Education.

Ajzen, Icec, & Albarracin, D. (2007). *Chapter 1: Predicting and Changing Behavior: A Reasoned Action Approach*. *Prediction and Change of Health Behaviour, Applying the Reasoned Action Approach*. NJ: Lawrence Erlbaum & Associates.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2011). Security policy compliance: User acceptance perspective. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3317–3326.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*.

Andress, & Jason. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practise* (2nd Editio). Amsterdam: Syngress.

Aurigemma, S., & Panko, R. (2011). A composite framework for behavioral compliance with information security policies. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3248–3257.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes*, *50*(2), 248–287.

Barua, A. (2013). Methods for decision-making in survey questionnaires based on Likert scale. *Journal of Asian Scientific Research*.

Boss, S., Kirsch, L., Angermeier, I., & Shingler, R. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of*.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548.

Cameron, J. (2006). *Rewards and intrinsic motivation: Resolving the controversy*.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, *29*(3), 157–188.

Coakes, S., Steed, L., & Ong, C. (2009). *Analysis without Anguish: SPSS version 16.0 for Windows*. Australia: John Wiley and Sons.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. *Research design Qualitative quantitative and mixed methods approaches* (4th Editio).

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of. *MIS Quarterly*, *13*(3), 319–340.

Draugalis, J. R., & Plaza, C. M. (2009). Best Practices for Survey Research Reports Revisited : Implications of Target Population , Probability Sampling , and Response Rate, *73*(8), 2–4.

Eisinga, R., Grotenhuis, M. Te, & Pelzer, B. (2013). The reliability of a two-item scale: Pearson, Cronbach, or Spearman-Brown? *International Journal of Public Health*, *58*(4), 637–642.

Fishbein, M. (2008). A reasoned action approach to health promotion. *Medical Decision Making*.

Furnell, S., & Clarke, N. (2012). Power to the people? the evolving recognition of human aspects of security. *Computers and Security*, *31*(8), 983–988.

Gollman, D. (2011). *Computer Security* (3rd Editio). Great Britain: John Wiley and Sons.

Goodhue, D., & Straub, D. (1991). Security concerns of system users: a study of perceptions of the adequacy of security. *Information & Management*.

Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Herold, R. (2011). *Managing an Information Security and Privacy Awareness and Training Program* (2nd Editio). Boca Raton: CRC Press.

Hill, D. G. (2009). *Data Protection. Governance, Risk Management and Compliance*. Boca Raton: Taylor and Francis Group.

Hinton, P., McMurray, I., & Brownlow, C. (2014). *SPSS explained*.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83–95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79.

Jager, W. (2003). Breaking bad habits: A dynamical perspective on habit formation and change. *Human Decision Making and Environmental Perception: Understanding and Assisting Human Decision Making in Real-Life Settings*.

Kerlinger, F., & Lee, H. (2000). *Foundations of behavioral research* (4th Editio). Orlandao: Harcourt College Publishers.

Kirsch, L., & Boss, S. (2007). The last line of defense: motivating employees to follow corporate security guidelines. *ICIS 2007 Proceedings*.

Komaki, J. (2003). *Reinforcement theory at work: Enhancing and explaining what employees do*. *McGraw-Hill* (7th ed.). Burr Ridge, IL: Irwin/McGraw-Hill.

Krejcie, R. V, & Morgan, D. W. (1970). Determining Sample Size for Research Activities Robert. *Educational and Psychological Measurement*, *38*(1), 607–610.

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

Liang, H., & Xue, Y. (2016). Ensuring Employees IT Compliance : Carrot or Stick ? Ensuring Employees ' IT Compliance : Carrot or Stick ?, *7047*(June 2013), 1–16.

Malaysia., & Lembaga Penyelidikan Undang-Undang. (2009). *Akta Aktiviti Kerajaan Elektronik 2007 (Akta 680) = Electronic Government Activities Act 2007 (Act 680) (hingga 5hb April 2009)*. International Law Book Services.

Malaysia, K. (2013). Personal Data Protection 2010. *Gazette*, 1–95.

MAMPU, Pekeliling Am Bil. 3 Tahun 2000 (2000).

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology*.

Merkow, M., & Breithaupt, J. (2005). *Information Security Principles and Practice*. New Jersey: Prentice Hall.

Metalidou, Marinagi, E., Trivellas, C., Eberhagen, P., & Giannakopoulos, N. (2014). Human Factor and Information Security in Higher Education. *Journal of Systems and Information Technology*, *16*(3), 210–221.

MyCERT. (2016). MyCERT Incident Statistics. Retrieved December 14, 2016, from https://www.mycert.org.my/statistics/2016.php

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection Motivation Theory. *Predicting Health Behaviour: Research and Practice with Social Cognition Models*.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10.

Pavlou, P., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*.

Peltier, T. R. (2004). *Information Security Policies and Procedures* (2nd Editio). United States of America: Auerbach Publications.

Podsakoff, P., Bommer, W., & Podsakoff, N. (2006). Relationships between leader reward and punishment behavior and subordinate attitudes, perceptions, and behaviors: A meta-analytic review of existing and new. *Behavior and Human*

Podsakoff, Philip, M., & Dennis, W. O. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management*, *12*(4), 531–544.

Rhee, H., Kim, C., & Ryu, Y. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*.

Richardson, R., & Director, C. (2008). CSI computer crime and security survey. *Computer Security Institute*.

Rogers. (2003). *Diffusion of Innovations*. *Free Press* (5th ed.). New York.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114.

Rogers, R. W., & Maddux, J. E. (1983). Protection Motivation and Self Efficacy: A Revised Theory of Fear Appeals and Attittude Change. *Journal of Experimental Social Psychology*, (19), 469–479.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65–78.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13.

Steers, R. M., Mowday, R. T., & Shapiro, D. L. (2004). Introduction to Special Topic Forum: The Future of Work Motivation Theory. *The Academy of Management Review*, *29*(3), 379.

Straub, D., & Welke, R. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53–55.

Tipton, H. F., & Krause, M. (2007). *Information Security Management Handbook* (6th Editio). Boca Raton: Auerbach Publications.

Turan, A., Tunç, A. Ö., & Zehir, C. (2015). A Theoretical Model Proposal: Personal Innovativeness and User Involvement as Antecedents of Unified Theory of Acceptance and Use of Technology. *Procedia -Social and Behavioral Sciences*, *210*, 43–51.

Tyler, T., & Blader, S. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal*.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198.

Venkatesh, V., & Davis. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46*(2), 186–204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology. *MIS Quaterly*, *27*(3), 425–478.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information*.

Whitman, M. E., & Mattford, H. J. (2012). *Principles of Information Security*. (J. Locke, Ed.) (4th Editio). Boston: Course Technology.

Workman, M., Bommer, W., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*.

Yunos, Z., Ahmad, R., Syahrul Hafidz Suid, & Ismail, Z. (2010). Safeguarding Malaysia's critical national information infrastructure (CNII) against cyber terrorism: Towards development of a policy framework. In *2010 Sixth International Conference on Information Assurance and Security* (pp. 21–27). IEEE.

Zhang, J., Reithel, B., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management &*.