USERS’ PERCEPTION OF THE INFORMATION SECURITY POLICY AT UNIVERSITI TEKNOLOGI MALAYSIA

HANIZA BINTI SHARIF

UNIVERSITI TEKNOLOGI MALAYSIA

USERS' PERCEPTION OF THE INFORMATION SECURITY POLICY AT UNIVERSITI TEKNOLOGI MALAYSIA

HANIZA BINTI SHARIF

A project report submitted in fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Centre for Advanced Software Engineering
Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

APRIL 2009

ACKNOWLEDGEMENT

First and foremost, I am deeply indebted to my supervisor, Dr. Zuraini Ismail for her patience in assisting, advising and guiding me throughout this project. Special thanks to my examiners, Associate Professor Dr. Zailani Mohamed Sidek and Dr. Rabiah Ahmad, for their comments and critics that make this study more comprehensive and precious. To admin staff of CASE, thank you for your continuous help and kind assistance during my presence in CASE.

To my family, a million thanks for your understanding and ardent support extended to me throughout my journey to accomplish this study, especially to my beloved husband who has been always standing by my side, understanding my hardships and accepting my weaknesses. Also, special dedication to all my kids: Din, Anur, Syafiq and Piqa, which I really hope that my achievement will also inspire them to grasp a fist of success in their future undertakings.

Lastly, thank you God for giving me strength to take up this challenge and with Your blessings, ‘Alhamdulillah’ I have managed to complete this study.

ABSTRACT

Securing information is essential for safeguarding the organization business operations as information is a business asset to any organization including education sector. One of the most imperative information security (InfoSec) controls identified is InfoSec policy. The purpose of this study is to gauge the level of enforcement and effectiveness of Universiti Teknologi Malaysia's (UTM) InfoSec policy from the users' perspective. This study involved three phases of data collection, namely preliminary study, interview and survey. The preliminary study allows an exploratory activity in understanding the information technology (IT) arrangement and organizational structural practices in UTM environment. Next, an interview with an IT-expert aimed to understand the establishment of the InfoSec in UTM. Then, a survey questionnaire is distributed to post-graduate and non-IT staff of UTM, *International Campus*, Kuala Lumpur to gauge the level of users' perception on the institution's security policy. The study had found that that nearly half of the users perceived that they are aware, understand and accept the UTM's policy, with more than half of the them agreed that the UTM's policy is effective. The study also proposed a theoretical framework model for the effectiveness of the institution's InfoSec policy. The model which consists of enforcement, users' awareness, users' understanding and users' acceptance identified as the independent variables, whereas an effectiveness of InfoSec policy identified as dependant variable. This proposed framework model may be useful as a basis for reference not only for researchers in this field but also for practitioner in developing the InfoSec policy.

ABSTRAK

Keselamatan informasi adalah penting bagi memastikan keselamatan operasi bagi setiap perniagaan kerana informasi merupakan asset utama bagi sesebuah organisasi termasuk sektor pendidikan. Polisi keselamatan informasi telah di kenalpasti sebagai salah satu kaedah yang berkesan bagi mengawal keselamatan informasi. Tujuan kajian ini dijalankan adalah bagi menilai tahap kepenggunaan dan keberkesanan polisi yang sediaada di Universiti Teknologi Malaysia (UTM) dilihat dari perspektif pengguna. Kajian ini dilaksanakan secara berperingkat iaitu peringkat permulaan, temuduga dan kajiselidik. Peringkat permulaan bertujuan untuk memahami perancangan IT serta carta organisasi yang sediaada di sekitar UTM. Peringkat kedua pula merupakan peringkat dimana pakar IT, UTM ditemuduga bagi mendapatkan gambaran sebenar polisi yang sediaada di UTM. Peringkat ketiga iaitu peringkat terakhir merupakan peringkat dimana soalan-soalan kajiselidik diberikan kepada para repondent yang terdapat di UTM, *International Campus*, Kuala Lumpur. Berdasarkan kajian yang dijalankan, didapati hampir sebahagian dari respondent sedar, faham, serta mengamalkan polisi ini. Kajian juga mendapati bahawa sebahagian dari respondent berpendapat bahawa polisi keselamatan yang sediaada adalah berkesan. Disamping itu, satu teori rangkakerja berkaitan dengan keberkesanan polisi keselamatan informasi untuk institusi pendidikan tinggi juga telah dicadangkan. Pembolehubah-pembolehubah yang dikenalpasti bagi rangkakerja ini termasuk faktor kesedaran, kefahaman dan penerimaan serta keberkesanan polisi ini. Rangkakerja ini diharap agar dapat membantu serta dibolehpakai bukan sahaja oleh pakar pengkaji keselamatan informasi malahan juga oleh para pengguna informasi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVIATIONS		DESCRIPTION
IS	-	Information Systems
IT	-	Information Technology
ICT	-	Information and Communication Technology
InfoSec	-	Information Security
IHL	-	Institution of Higher Learning

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Developments in Information and Communication Technology (ICT) certainly have impacted all sectors such as banking, insurance, private organization, health, transportation, military and government. The education sector, particularly institutions of higher learning (IHL) is also not spared. As computer usage becomes more and more pervasive (Al-Salihy et al., 2003), it provides the ability for the institutions to automate, adapt and accelerate their learning strategies (Bakari et al., 2005).

The modern world thrives on information and its flows; the contemporary world, society, and institutions cannot function without their computer-communication-based information system (Pfleeger et al., 2007). The effect from this situation had exposed the information system to probable threats and risks. Hence, these systems must be protected from all aspects; technical, procedural, operational and environmental. Thus, a safe and secure information environment is vital to the organizations. Information system must provide information with the highest possible level of integrity, availability and confidentiality. Therefore, various controls and measures have been taken and implemented by various organizations in the world including Malaysia.

The Malaysian Communications and Multimedia Commission, a statutory body had been set up under the Malaysian Communications and Multimedia Commission Act 1998 to be responsible for overseeing the telecommunications, broadcast and online activities for various sectors in the country including financial sector, military, transportation, government office and to-date education sector. Besides, having information security policy is one of the most vital security controls identified and necessary for any organizations. This vital direction-giving documents is, however, not always easy to develop and implement.

1.2 Background of the Problem

Information is a business asset that has value to any organizations including IHL. Securing information is a critical issue threatening organizations worldwide. Security covers many different areas such as physical, network, platform, communication and application; and each area has its own risks, threats, and definitely solutions. The survey on the attacks and security incidents reported by MyCERT, CyberSecurity Malaysia (CyberSecurity, 2008) for the first quarter (Q1) 2008 revealed that a total of 10,354 security incidents inclusive of spam incidents were reported. This represented an increase of 5.59% incidents rate compared to fourth quarter (Q4) in 2007. The categories of incidents identified are intrusion, hack threat, malicious code, denial of service and spam.

According to Wayne (1993) the computer crimes are almost inevitable in any organizations in Malaysia currently unless adequate protections are put in place. The top most three computer's crimes identified are computer viruses, natural disaster and negligence. These crimes had inevitably caused a total of 17,712 cases of bank fraud involving RM124.13 million between 1986 and 1992. The total estimated losses due to computer crime worldwide ranges from $300 million to $500 billion per year for the same period of year. Lack of awareness on the vulnerable of data, software and hardware amongst users has been identified as the main cause of the crime.

In United States (US), the academic institutions had faced InfoSec threats and severe breaches (Steffani, 2006). Incidents such as information theft, data tampering, viruses, worms and terrorist activity constitute significant threats to public safety and national security. Despite these InfoSec issues, however, only a few researches have been conducted pertaining to the policy, practice and theoretical levels to address the issues. Basically, the goal of the study is know the level of knowledge, policy and practices of individuals and organizations regarding institution's (InfoSec).

Information Security (InfoSec) policy is an organization document that outlines the security requirements or rules that must be met (SANs, 2008b) and adhered by the organization with the intention to reduce risk, security incidents and minimize the effect including cost and resources. Reviews of three Malaysian institutions of higher learning's websites disclose that basically the institutions have the InfoSec policy. Unfortunately, different institution has different set of policy. For example, one of the institutions had focused on the administrative issue of managing the computer laboratory and password while the other institution covered only the networking and communication. In addition, a review on seven other foreign universities' websites located in the United Kingdom and the United States had also revealed that the focus of the established policies is different amongst the universities.

Journals listed in the Malaysian Journal of Computer Science's website (MJCS, 2008), University of Malaya, shows that there are 278 journals produced between years of 1985 to 2008. However, the journals are focusing more on technical and general perspective of network, communication, application and internet. Unfortunately, users' awareness and enforcement of the InfoSec policy are less discussed and presented in the journals.

.

1.3 Problem Statement

Securing information is essential to any organization for safeguarding the information system from any security breaches or incidents. There are many ways the organization can implement in order to secure the information such as from technical, physical, or operational environment's perspective. Realizing that the InfoSec policy is one of the most crucial security controls in securing the information system, thus, having effective InfoSec policy is vital for any organization. By definition, policy is a set of management instructions indicating a course of action, mandatory and can be though as equivalent of an organization specific law (SANs 2008b). Therein, the policy is crucial to discipline and ensure that the staff comprehending the management needs with regards to securing the business asset. Thus, having comprehensive security programme such as well documented policy, and proper enforcement of the policy will enhanced the security control of the information. This subsequently will reduce the risks of business or information being attacks or having security incidents.

An analysis of the InfoSec policy literature had addressed the following gaps:

i. A tremendously increase in the number of security incidents and attacks to the business operations especially in Malaysia recently had provide warrant to most organization including IHL that necessary steps need to be taken to evade these incidents. The security incidents may be precipitated by disgruntled or dishonest employees. Even the lack of awareness on the management of password such as passwords posted on monitors can put the entire information technology system of the institution at risk. Thus, the study on the state of enforcement which covers the users' awareness, understanding and acceptance of this established InfoSec policy may helps the IHL to gain basic understanding on the level of the security strength at their institution.

ii. Though the academic institutions had faced InfoSec threats and severe breaches, however, only a few researches have been conducted pertaining to the policy, practice and theoretical framework levels to address the issues (Steffani, 2006).

iii. The absence of a standard InfoSec policy framework adopted by IHL particularly in Malaysia. Currently, different IHL adopted different set of security policy.

iv. Lack of journals or reports produced in Malaysia that covering the InfoSec policy particularly related to IHL. Most of the journals covering areas related to internet and website particularly on public sector. This study expected to provide information related to InfoSec policy for IHL.

1.4 Project Objectives

The objectives of this study are as follows:

- To investigate the status of InfoSec policy for Universiti Teknologi Malaysia (UTM);

- To identify components that constitute UTM's InfoSec policy; and

- To examine the level of enforcement and effectiveness of UTM's InfoSec policy.

1.5 Project Aim

The aim of this study is to investigate the status and to examine the enforcement of the InfoSec policy in the IHL in Malaysia, particularly in UTM from the users' perspective. The outcome of this study can be used as a proposal for the development of a standard InfoSec policy framework which may be suggested to other institutions for a better security management practice within the IHL community in Malaysian context.

1.6 Project Scope

The scope for this study is to investigate the status and to examine the enforcement and the effectiveness of InfoSec policy in UTM environment from the users' perspective.

1.7 Summary

The chapter begins with an overview of the importance of ICT and the implication to various sectors including education sector, and followed by the background of the problem. The issues on lack of information related to enforcement of InfoSec policy and increasing number of security incidents and computer crimes especially in the education sectors have led to the problem statement subsequently defining the project objectives. The project's aims and scope were then discussed.

The next chapter presents the review of the InfoSec policy literature.

REFERENCES

Al-Salihy, W., Ann, J., and Sures. R. (2003). Effectiveness of Information Systems Security in IT Organizations in Malaysia. *Proceedings of 9th Asia-Pacific Conference on Communication*, 21-24 Sept 2003.

Bardin, J. (2008). A Standard, a Framework or a Standard Framework? *CSO, Security & Risk*. Retrieved on August 10, 2008, from: http://blogs.csoonline.com/a_standard_a_framework_or_a_standard_framework.

Bakari, J.K., Tarimo, C.N., Yngstrom, L., and Magnusson, C. (2005). State of ICT security management in the institutions of higher learning in developing countries: Tanzania case study. *Fifth IEEE International Conference on Advanced Learning Technologies, ICALT 2005*. 5-8 July 2005.

BSI (1999). *BS7799 Code of Practice for Information Security Management Information.* Security, Audit and Control Association British Standards Institution. ISACA. July 2000.

Canavan, S. (2003). *An Information Security Policy Development Guide for Large Companies*. The SANS™ Institute 2001.

CyberSecurity (2008). *E-Security: MS-125.022008:* MyCERT Quarterly Summary (Q1)2008, *Cyber Security Malaysia.* April 2008. Retrieved on September 17, 2008, from: http://www.cybersecurity.my/data/content_files/12/382.pdf?.diff=12155750.

COBIT (2008). 3rd Edition Control Objectives. *ISACA*. Retrieved on September 15, 2008, from: http://www.isaca.org.

Cooper, D. (2003). Psychology, risk & safety: understanding how personality & perception can influence risk taking. *Professional Safety.* Pp 39–46 (2003).

Cooper, D. R., and Schindler, P. S (2008). *Business Research Methods.* Mc Graw Hill, International Edition.

DesPlanques, D. (2005). *Information Security Policy Development for Institutions of Higher Education.* Thesis for Master. Regis University, School for Professional Studies. 2005. Retrieved on October 14, 2008, from: http://www. academic.regis.edu/cias/ia/DesplanquesProfessionalProject.doc.

EDUCAUSE (2004). Information Security Governance Assessment Tool for Higher Education. Boulder. *Security Tasks Force, EDUCAUSE, Colorado and Washington,* D.C. Retrieved on November 20, 2008, from: http://connect.educause.edu/Library/Abstract/InformationSecurityGovern/43206?time=1237881590.

Gonzalez, J.J., and Sawicka, A. (2002). A Framework for Human Factors in Information Security. *WSEAS* – Presented at the 2002 WSEAS Int. *Conf. on Information Security, Rio de Janeiro,* 2002.

Hinde, S. (2002). Security Surveys Spring Crop. *Computers and Security*, Vol. 21, No. 4, pp. 310-321.

Hone, K., and Eloff, J.H.P. (2002). What makes an Effective Information Security Policy. *Network Security*, Vol. 20, No. 6, pp. 14-16.

Hone, K. (2004). The Information Security Policy – An Important Information Security Management Control. (Degree Dissertation, Rank Afrikaans University, 2004). *Dissertation of Mcom (Informatic), Faculty of Economic and Management Science.*

Huang, DL., Rau, PL. P., and Salvendy, G. (2007). *Survey of Factors Influencing People's Perception of Information Security.* Springer Berlin / Heidelberg. Volume 4553/2007.

ISP (2009). Information Security Policy Objectives. *Information Security Policy World. The Security Policies & Standards Group, London.* Retrieved on January 15, 2009, from: http://www.information-security-policies-and-standards.com/objective.html.

ISF (2003). The Forum's Standard of Good Practice in March 2003. *Information Security Forum.* Retrieved on November 15, 2008, from: http://www.isfsecuritystandard.com.

IBM (2008). *IBM Information Security Framework*. IBM, USA. Retrieved on October 10, 2008, from: http://www. ibm.com/services/security.

Jilly, S., and Andy, K. (2006*). Information Technology Security & Risk Managemen*t. John Wiley & Sons Australia, Ltd.

Joy, R. H., and Jack, S. (2005). *Presidents and Campus Cybersecurity* EDUCAUSE Review, vol. 40, no. 6 (November/December 2005). Retrieved: September 4, 2008, from: http://connect.educause.edu/Library/EDUCAUSE+Review/SafeguardingInformationAs/40662?time=1220399448he CSO.

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* (2003). ISSN 0268-4012.

Kee, C.K. (2001). Security Policy Roadmap – Process for Creating Security Policies. *The SANS™ Institute 2001.*

Kark, K., Orlowv, L.M., and Bright, S. (2006). *How to Manage Your Information Security Policy Framework.* Retrieved: August 20, 2008, from: http://www.forrester.com/Research/Document/Excerpt/0,7211,38615,00.html

KPM (2008). Bahagian Teknologi Maklumat and Komunikasi, *Kementerian Pelajaran Malaysia.* Retrieved on July 16, 2008, from: http://www.mohe.gov.my/web_statistik/index.htm?navcode=NAV038?m=3&navcode=NAV038&subcode=SUB001&lang=ENG.

Krutz, R.L., and Vines, R.D. (2001). *The CISSP® Prep Guide – Mastering the Ten Domains of Computer Security*. John Wiley & Sons, Inc.

Madigan, E. M., Petrulich, C., and Motuk, K. (2004). The cost of Non-Compliance - When Policies Fail. *Proceedings of the 32nd annual ACM SIGUCCS conference on User services,* pp. 47 – 51, USA.

MJCS (2008). Malaysian Journal of Computer Science. *MyAIS Faculty of Computer Science and Information Technology, University of Malaya* (1985-2008). Retrieved: July 25, 2008, from: http://myais.fsktm.um.edu.my/view/type/article/Malaysian_Journal_of_Computer_Science.html.

Maria, K., Evangelos, K., and Spyros, K. (2004). Information systems security policies: a contextual perspective.Computers & Security Volume 24, Issue 3, May 2005, pp 246-260.

Norashikin, Sharif (2007). *Conceptualising And Developing Information Secuirty Awareness And Training Programme. Case Study: Malaysian Financial Sector. Master Thesis,* CASE, Universiti Teknologi Malaysia.

Noran Fauziah, Yaakub and Ahmad Mahdzan, Ayob (1999). H*igher Education and Socioeconomic Development in Malaysia: A Human Resource Development Perspective*. Doctor Philosophy, Universiti Utara Malaysia.

Nosworthy, J.D. (2000). Implementing Information Security in the 21st Century – Do You Have the Balancing Factors? Computers & Security, 19(4), pp.337– 347.

Pfleeger, C.P., and Pfleeger, S.L. (2007). *Security in Computing.* (4th ed): Pearson Education, Inc (Pearson International Edition).

Poore, R. S. (2001). Generally Accepted Systems Security Principles. *International Information Security Foundation.* Retrieved: November 20, 2008. from: http://www.infosectoday.com/Articles/gassp.pdf.

Rees, J., Bandyopadhyay, S., and Spafford. E. H. (2003). A Policy Framework for Information Security. *CERIAS Tech Report 2003-35, July 200 3, Vol. 46, No. 7 Communications of the ACM.*

RDSU (2008). *Qualitative Research Methods.* Peninsular Research & Development Support Unit, UK. Retrieved on November 12, 2008, from: http://projects.exeter.ac.uk/prdsu/helpsheets/Helpsheet09-May03-Unlocked.pdf.

Rothke, B. (2005). Computer Security: 20 Things Every Employee Should Know. *McGraw-Hill.* ISBN: 0072262826.

Sandy, B. (2008). Building an Effective Information Security Policy Architecture. *Publisher CRC,* Rating, page 340.

Salvendy, G. (1997). *Handbook of Human Factors and Ergonomics.* Wiley-Interscience, Chichester.

Stephen P. B. (1996). *Theoretical Framework.* Retrieved on January 3, 2009. From: http://www.analytictech.com/mb313/elements.html.

Steffani A. B. (2006). The Impact of Information Security in Academic Institutions on Public Safety and Security: Assessing the Impact and Developing Solutions for Policy And Practice. *Report for Department of Justice, US.* Retrieved on October 3, 2008, from: http://dx.doi.org/10.3886/ICPSR21188.

SANs (2008a). A Short Primer for Developing Security Policies. *The SANS Institute.* Retrieved on September 20, 2008, from: http://www.sans.org/resources/policies/Policy_Primer.pdf.

SANs (2008b). IT Security Policies. *The SANS Institute* 8120 Woodmont Avenue, Suite 205 Bethesda, Maryland. Retrieved on September 20, 2008, from: http://www.sans.org/resources/policies.

Tittel, E., Chappel, M., and Stewart, J.M. (2003). *CISSP® Certified Information Systems Security Professional Study Guide.* Sybex, Inc. ISBN 0-7821-4175-7.

Tiwana, A. (1999). *Web Security*. Digital Press. ISBN 1 -55558-210-9.

Tudor, J. K. (2001). *Information Security Architecture: An Integrated Approach to Security in the Organization*. *CRC Press LLC*. ISBN 0-8493-9988-2.

Ungerman, M. (2005). Creating and Enforcing an Effective Information Security Policy. *Information Systems Control Journal*, volume 6, ISACA®, Inc.

VanCura, L. (2005). Building a Security Policy Framework for a Large, Multi-national Company. © *SANS Institute 2005.*

Varmey, C. A. (1996). Consumer Privacy in the Information Age: A View from the United States. *Remarks before the Privacy and American Business National Conference, Washington.*

Vyskoc, J., and Fibikova, L. (2001). IT users' perception of information security. *2nd Working Conference on Security and Control of Information Technology in Security 2001*, Comenius Univ., Bratislava, Slovakia.

Wayne, C. S. (1993). Computer Security in Malaysia. *Proceedings of the National in Information Technology, Kuala Lumpur, Malaysia. September 1993. R*etrieved on October 2, 2008, from: http://csc.colstate.edu/summers/research/docs/COMP-SEC.A14.html.