AWARENESS AND ACCEPTANCE ANALYSIS OF INFORMATION SECURITY POLICY

MOHD ZUKI BIN MUDA

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

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

MARCH 2010

ABSTRACT

Today the Armed Forces around the world face a fast and radical change towards digitalisation. This is including Malaysian Armed Forces. Therefore it is essential for the Malaysian Armed Forces to safeguard their information from been accessed by unauthorised personnel. One of the most significant information security controls is information security policy. The purpose of this research is to evaluate the level of awareness and acceptance of the Malaysian Armed Forces Information Security Policy. The study has proposed a research model for the effectiveness of the policy. The components of the research model consist of management support, users' acceptance, enforcement and revision. Interview and survey has been used to collect the data based on the model. The interview was conducted to investigate the status of the policy while the survey was conducted to evaluate the level of awareness and acceptance of the Malaysian Armed Forces Security Policy among the Armed Forces personnel. The respondents for this study involved the personnel of Information Technology Department of the Armed Forces namely Information Technology Department of Army, Information Technology Department of Navy and Information Technology Department of Air Force. The findings showed that the majority of the Armed Forces personnel are agreed that they are aware of the existence of the policy and exhibit agreement to the policy. A majority of the respondents agreed that the policy is effective and can assist the military to achieve their main role to protect the sovereignty of nation. This study would be useful for the management of the Armed Forces as well as the practitioner to develop and manage the information security policy.

ABSTRAK

Pada masa ini angkatan tentera di seluruh dunia mengalami perubahan cepat dan radikal menuju ke arah pengkomputeran. Ini tidak terkecuali Angkatan Tentera Malaysia. Justeru itu adalah satu kemestian bagi Angkatan Tentera Malaysia memastikan maklumat mereka tidak dicapai oleh pihak luar. Salah satu cara kawalan yang paling penting ialah mewujudkan polisi keselamatan maklumat. Objektif kajian ini adalah untuk menilai tahap kesedaran dan penerimaan anggota Angkatan Tentera Malaysia terhadap Polisi Keselamatan Maklumat Angkatan Tentera Malaysia. Penyelidikan ini telah mencadangkan satu model penyelidikan untuk keberkesanan polisi ini. Model penyelidikan ini mengandungi komponen sokongan pengurusan, penerimaan pengguna, penguatkuasaan dan menilai semula. Temuduga dan tinjauan telah digunakan untuk mengumpul data. Temuduga dilakukan untuk menyiasat status dasar sementara tinjauan dilakukan untuk menilai tahap kesedaran dan penerimaan anggota Angkatan Tentera Malaysia ke atas polisi keselamatan maklumat. Responden untuk temuduga telah meliputi anggota Jabatan Teknologi Maklumat daripada Tentera Darat, Tentera Laut dan juga Tentera Udara. Penemuan menunjukkan majoriti anggota Angkatan Tentera Malaysia bersetuju bahawa polisi sedia ada adalah berkesan dan boleh membantu Angkatan Tentera mencapai peranan utamanya menjaga kedaulatan negara. Penemuan ini penting untuk pengurusan Angkatan Tentera dan juga pakar-pakar keselamatan maklumat untuk membangun dan mengurus polisi keselamatan maklumat.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVIATIONS		DESCRIPTION
BS	-	British Standard
C4ISR	-	Command, Control, Communications, Computers, Intelligence and Reconnaissance
CobiT	-	Control Objectives for Information and Related Technology
EISP	-	Enterprise Information Security Policy
IEC	-	International Electrotechnical Commission
ISO	-	International Organisation for Standardization
IT	-	Information Technology
NIST	-	National Institute of Standards and Technology
SAS	-	Statistical Analysis Software
SETA	-	Security Education Training and Awareness
SPF	-	Security Policy Framework
TCSEC	-	Trusted Computer System Evaluation Criteria
UTM	-	Universiti Teknologi Malaysia

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Computer information systems and telecommunication systems are technologies that every organization uses in their daily pursuit of business. Organizations are more dependent than ever on the reliable operation of their information system (Knapp *et al*., 2009).

Therefore a safe and secure computing environment is vital to any organizations. Information system must provide information with the highest possible levels of integrity, availability, and confidentiality. Thus, various controls and measures have to be implemented in organizations. Undoubtedly the singularly most important of these controls is the information security policy (Knapp *et al*., 2009).

1.2 Background of the Problem

Most of the organization relies on information systems in pursuit of their daily business. Dependence on information systems and services means organizations are more vulnerable to security threats. Then, the interconnecting of

public and private networks and sharing of information resources increases the difficulty of achieving access control. The trend towards distributed computing has weakened the effectiveness of central, specialist control (ISO/IEC 27002, 2005).

As information is an asset to any organization, securing information is a critical issue threatening organizations worldwide. Increasingly, organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common more ambitious and increasingly sophisticated.

According to a statement given by Chief Executive Officer of Cyber Security, Lt Col (R) Hussin bin Jazri, the number of cybercrimes reported to them had more than doubled in 2008 compare to 2007 (Jazri, 2009). In 2008, Cyber Security handled a total of 2,123 incidents which is higher than a 100% increase compared to 2007 when they handled 1,038 incidents. Almost half of the reported incidents involved fraud and the remainder were about intrusions and malicious code.

Lt Col (R) Husin added, with the increase of wireless and broadband capability make it easier and faster to use internet. And at the same time it will encourage more country's cyber population, the number of online transactions or other activities will increase in tandem, which will likely mean more incidents of cybercrime. Currently, there are 13.5 million Internet users in the country today and the number is increasing. They will use this facility as well to conduct their crimes online. The current economic situation, in which the global economy is heading towards a recession, will also contribute to an increase in cybercrimes. These all incidents involved the non military organisations.

There are no exceptions to Armed Forces around the globe where their computer systems have been hacked. In 1997, two California teenagers and a trio of Israeli hackers were arrested for hacking into Pentagon servers. Then 2002 Gary

McKinnon, a 36-year-old former systems administrator from London, was charged by a grand jury in New Jersey with intentionally damaging a federal computer system, according to a statement released by the US Attorney's Office in the Eastern District of Virginia. McKinnon is believed to have attacked the Earle Naval Weapons Station, a US Navy command centre responsible for supplying munitions to the Atlantic fleet, three times between April 2001 and September 2001 (Kane, 2002).

Therefore, in order to safeguards computer systems it is mandatory for any organisation to have an effective Information Security Policy. Information Security Policy acts as first layer of defence to security threats (Whitman and Mattord, 2008).

1.3 Problem Statement

Security policy is a high level statement of organizational beliefs, goals and objectives and the general means for their attainment as related to the protection of organizational assets. In brief, it is set at a high level and never states “how” to accomplish the objectives (Abdul Hamid, 2007). The primary goal of the security policy is to prevent or minimize the loss of assets or resources due to security breach.

In Malaysian Armed Forces environment, although the information security policy is already in place but the lack of monitoring, security education, training, awareness programs and enforcement the possibility of security breach is there. Do not forget that the threat is not only from external it is also can come from internal as well. One of the mechanisms to measure the level of awareness and acceptance of Armed Forces Personnel toward Armed Forces Information Security Policy the survey should be conducted.

1.4 Project Aim

The aim of this study is to investigate the status of Malaysian Armed Forces Information Security Policy and measure the level awareness and acceptance of the Policy. The outcomes of this study can be used by Cyber Warfare Division as guidance to conduct security programs to Armed Forces personnel.

1.5 Project Objectives

The objective of the study as follows:

a. To investigate the status of Malaysian Armed Forces Information Security Policy.

b. To identify components that constitutes Malaysian Armed Forces Information Security Policy.

c. To evaluate the level of awareness and acceptance of the Malaysian Armed Forces Information Security policy.

1.6 Project Scope

The scope for this study covers the investigation on the status of Armed Forces Information Security Policy, level of awareness and acceptance of Armed Forces Security Policy by Armed Forces personnel.

1.7 Significance of the Study

Most of organisations claim to have formulated and implemented information security policy but still have security breaches in their organisation. This is may be because the organisation never measures whether their information security policy is well accepted by their employees or worse still employees may not even know about the existence of the policy itself. As a result, they do not know how effective their information security policy is?

One potential explanations as to the apparent ineffectiveness of information security policy is that they adopt a very narrow definition of information security policy which only focus upon issues of information confidentiality, integrity and availability (Dhillon and Backhouse, 2000). Therefore, one way of measuring the effectiveness of an information security policy is by conducting a survey.

1.8 Summary

Information security is very important to all organisations including military, public and private. Information security can be achieved by implementing sets of control. One of the most important information security controls is the information security policy (Hone and Eloff, 2002). Information Security Policy should be established, implemented, monitored, reviewed, improved and enforced.

REFERENCES

Abdul Hamid, R., (2007). *What You Need To Know About Security Policy?* Retrieved on Jan 10, 2010, from: http://www.cybersecurity.my/data/content_files/11/53.pdf?.diff=1176336999.

Alzak, T., (2009). Security Basics - Components of Security Policies. Retrieved on September 13, 2009 from: http://www.brighthub.com/computing/smb-security/articles/2259.aspx

Bishop, M. (2003). What is computer security?. In *IEEE Security & Privacy*. pp. 67–69.

Brewer, D. F. C. and Nash, M. J. (1989): „The Chinese Wall Security Policy". In: *Proceedings of the 1989 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press pp. 206–214.

David, J. (2002). Policy Enforcement in the Workplace. Computers & Security 21(6), pp. 506-13.

Davis, GB, Olson MH (1985). Management Information Systems - Conceptual Foundations, Structure and Development. 2nd ed. New York: McGraw-Hill Book Company; 1985.

Dhillon,G., and Backhouse,J. (2000),Information System Security Management in the New Millennium, Communications of the ACM, volume 43, number 7, pp. 125-128.

Doherty, N. F, Anastasakis, L. and Fulford, H. (2009a): The Information Security Policy Unpacked: A Critical Study of the Content of University Policies. In: *International Journal of Information Management*.

Doherty, N. F. and Fulford, H(2006): Aligning the Information Security Policy with the Strategic Information Systems Plan. In: *Computers & Security*. 25 (1), pp. 55-63.

Ferraiolo, D.F. & Kuhn,D.J.,1992. Role-Based Access Controls. In 15th National Computer Security Conference. pp. 80-90.

Gaston, S.J. (1996). Information Security: Strategies for Successful Management. Toronto: CICA.

Gollmann,D. (2006). *Computer Security 2nd Ed*, John Wiley & Sons Ltd, West Sussex, England.

Higgins,H.N.(1999). Corporate System Security: Towards an Integrated Management Approach. *Information Management and Computer Security,7(5),* pp. 217-222.

HMG (2009). *HMG Security Policy Framework*. HMG Office.
Retrieved on Feb 18,2009, from:
http://www.cabinetoffice.gov.uk/media/hmg_security_policy.pdf

Holzinger,A. (2000). Information Technology Management and Assurance - A call to Action for Corporate Government, *Information System Security,* May/June, volume 9, Issue 2.

Höne, K. & Eloff, J.H.P., (2002a). What Makes an Effective Information Security Policy? *Network Security*, Volume 6, pp. 14-16.

Hone, K. and Eloff, J.H.P. (2002b). Information Security Policy — What do International Information Security Standards Say? *Computers & Security*, 21(5), pp. 402-409.

Hong, K., Chi, Y., Chao, L.,&Tang, J. (2006). An Empirical Study of Information Security Policy on Information Security Elevation on Taiwan. Information Management and Computer Security, 14(2), pp.104–115.

ISO/IEC 17799 (2000), *Information Technology – Code of Practice for Information Security Management*, International Organization for Standardization (ISO).

ISO/IEC 27002 (2005), *Information Technology – Code of Practice for Information Security Management*, International Organization for Standardization (ISO).

Jazri, H., (2009). *Cybercrimes Analysis.*
Retrieved on Jan 11, 2010, from:
http://www.cybersecurity.my/ en/media_centre/press_release/2009/
612.pdf?.diff=1262084879

Kane, M., (2002). *British Man to be Extradited for US Military Hacks.* Retrieved on Jan 5, 2010, from: http://news.zdnet.co.uk/security/0,1000000189,2125830,00.htm .

Karyda, M., Kiountouzis, E., and Kokolakis, S. (2005), Information systems security policies: a contextual perspective, *Computers and Security*, Volume 24,pp. 246-260.

Kessler, G. C. (2001): Nontechnical Hurdles to Implementing Effective Security Policies. In: *IT Professional*. 3 (2), pp. 49–52.

Knapp, K. J; Franklin Morris, R. and Marshall, T. E; et al. (2009): Information Security Policy: An organizational-level Process Model. In: *Computers & Security*.

Lee, R.D., (2001). *Developing Effective Information Systems Security Policies* Retrieved on January 5, 2010, from: http://www.sans.org/reading_room/whitepaper/policy/developing_effective_information_systems_security_policies.

Longman, (2005). *Longman Dictionary of Contemporary English.*

Marcinkowski, S. and Stanton, J., (2003). Motivational Aspects of Information Security Policies. In *Systems, Man and Cybernetics, 2003. IEEE International Conference on*. pp. 2527-2532 vol.3.

Nnolim,A.L., (2007). A Framework and Methodology for Information Security Management. Doctor Philosophy, Lawrence Technological University, Michigan.

NIST SP 800-80. (2006). Guide for Developing Performance Metrics for Information Security.

Peltier, T. R. (2002), *Information Security Policies, Procedures, and Standards – Guidelines for Effective Information Security Management*, Auerbach Publications, Boca Raton, Florida.

Perks and Beveridge, (2003). Guide to Enterprise IT Architecture,Springer Verlag, Houston.

Posthumus, S. & von Solms, R., 2004. A Framework for the Governance of Information Security. *Computers & Security*, 23(8), 638-646.

Rees, J., Bandyopadhyay, S. and Spafford, E. H. (2003), PFIRES: A Policy Framework for Information Security, *Communications of the ACM*, July, Volume 46, Number 7, pp. 101-106.

Robitschek, R., (2001). *Manage your Security Initiative as a Project*. Retrieved on Dec 10,2009, from http://www.sans.org/reading_room/whitepapers/

Rungta, S., Raman, A., Kohlenberg, T., Li, H., Dave, M., & Kime, G. (2004), Bringing Security Proactively into the Enterprise, *Intel Technology Journal*, Volume 8, Issue 4, pp. 303–311.

Russell, D and Gangemi, G.T. (1991). Computer Security Basic. 1st Edition, CA.: O'Reilly & Associates Inc.

Saint-Germain, R., (2005). Information Security Management Best Practice Based on ISO/IEC 17799. *Information Management Journal - Prairie Village, volume* 39(4), pp. 60.

Saleh, M.S., Alrabiah, A., and Saad, H. B. (2007). Using ISO 17799; 2005 Information Security Management: A STOPE View With Six Sigma Approach. International Journal of Network Management, 17(1), pp. 85–97.

Schwarz, N. & Oyserman, D.,(2001). Asking Questions about Behavior: Cognition, Communication, and Questionnaire Construction. *American Journal of Evaluation*, 22(2), 127.

Sharif, H., 2009. User's Perception of the Information Security Policy at Universiti Teknologi Malaysia. Master of Computer Science (Information Security), Universiti Teknologi Malaysia.

Shield, (2009). *Policy Research – Eight Elements of Effective Information Security Policies.* Retrieved on Dis 15, 2009, from: http://whitepaper.windowsecurity.com/

Shim, J. K., Qureshi, A. A. and Siegel, J. G. (2000). The International of Computer Security. 1st Edition. Chicago,: GPCo.

Simon H.A.,(1957). *Administrative Behavior*. 2nd ed. New York:The Free Press.

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

von Solms, B., and von Solms, R. (2004), The 10 deadly Sins of Information Security Management, *Computers and Security*, Volume 23, pp.371-376.

Whitman, M. E. and Mattord, H.J., (2008). *Management of Information Security*. 2nd Edition. Boston, MA,: Course Technology.

Yip, F., Ray, P. and Paramesh, N., (2006). Enforcing Business Rules and Information Security Policies through Compliance Audits; XISSF - A Compliance Specification Mechanism. In *Business-Driven IT Management, 2006. BDIM '06. The First IEEE/IFIP International Workshop on*. pp. 81-90.