STUDY ON INFORMATION SECURITY AWARENESS AMONG STAFFS

MALIHE MOTIEI

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Information Technology- Management)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

MARCH 2012

Dedicated to my beloved family especially, husband, lovely daughter Aida, my parents and my supportive supervisor Dr. Mohd Shahizan Othman. Thank you very much for being supportive, helpful and understanding.

ACKNOWLEDGEMENT

In the Name of Allah, Most Gracious, Most Merciful

First and foremost, I would like to express heartfelt gratitude to my supervisor Dr. Mohd Shahizan Othman for his constant support during my study at UTM. He inspired me greatly to work in this project. His willingness to motivate me contributed tremendously to our project. I have learned a lot from him and I am fortunate to have him as my mentor and supervisor

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities.

ABSTRACT

These days, as increasing the number of internet users, numbers of hackers and intruders is also increasing. There also is essential need to improve information security of organizations. One of the main parts of information security issue is awareness of employees about new threats and vulnerability points. Hence the organizations have often established the programs to increase the information security awareness. So the level of awareness can be an important measure to help top management and information security department for developing a new security awareness program. In this research the security awareness of staff was studied and measured. Scope of the study is to make a survey for knowing thoughts of staff about information security. We did a survey in CICT department to reach objectives. Dean of CICT and security team are interviewed to provide the necessary information. They have been asked questions about how they work to raise the security awareness and improve the attitudes among their employees and also how they measure the level of information security awareness among staff. According to the interview session with the dean of the CICT there is no staff's information security awareness survey was conducted before. This study can be as original study. The main purpose of this study is to help the information security management to know what the level of security awareness among staffs is. The results from this study can also be used as additional information when improving or planning university's information security system.

ABSTRAK

Kini, boleh dilihat pertambahan bilangan dari segi pengguna internet, penggodam dan juga penceroboh yang semakin berleluasa. Terdapat juga keperluan penting untuk meningkatkan keselamatan maklumat sesebuah organisasi. Salah satu bahagian utama isu keselamatan maklumat adalah kesedaran pekerja tentang ancaman baru dan titik kelemahan. Oleh itu organisasi telah sering mewujudkan program-program untuk meningkatkan kesedaran keselamatan maklumat. Jadi, tahap kesedaran boleh menjadi satu daripada langkah penting untuk membantu pengurusan pihak atasan jabatan keselamatan dan maklumat untuk membangunkan satu program baru berkenaan dengan kesedaran keselamatan. Dalam kajian ini kesedaran keselamatan kakitangan akan dikaji dan diukur. Skop kajian ini adalah untuk membuat kaji selidik bagi mengetahui pemikiran kakitangan tentang keselamatan maklumat. Kami sedang melakukan satu kajian di jabatan CICT untuk mencapai objektif tersebut. Dekan CICT dan pasukan keselamatan telah ditemu bual untuk menyediakan maklumat yang diperlukan. Mereka telah ditanya soalan tentang bagaimana mereka bekerja untuk meningkatkan kesedaran keselamatan dan memperbaiki sikap di kalangan pekerja-pekerja mereka dan juga bagaimana mereka mengukur tahap kesedaran keselamatan maklumat di kalangan kakitangan. Menurut sesi temuduga dengan Dekan CICT, tiada lagi kajian berkaitan dengan maklumat kesedaran keselamatan yang dijalankan sebelum ini. Justeru itu, kajian ini boleh menjadi sebagai rujukan kajian asal. Tujuan utama kajian ini adalah untuk membantu pengurusan keselamatan maklumat bagi mengetahui tahap kesedaran keselamatan di kalangan kakitangan. Hasil daripada kajian ini juga boleh digunakan sebagai maklumat tambahan apabila memperbaiki atau merancang sistem keselamatan maklumat universiti.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CIA	Confidentiality, Integrity, Availability
InfoSec	Information Security
SE	Social Engineering
IAV	Information Availability
NOC	Network Operation Center
FTP	File Transfer Protocol
IS	Information System
ISO	International Standard Organization
ICT	Information Communication technology
CICT	Center for Information and Communication technology

CHAPTER 1

INTRODUCTION

1.1 Introduction

With today's advance and widely accessible communication technologies information security is a significant topic for protecting the organizations against intruders. Information security awareness among staff also plays an effective role for protecting information. Hence, level of information security awareness is defined as one of the main concern in this area. So, researchers have proposed own techniques for increasing awareness among employees. (Adam-mark, 1975; Mathisen, 2004; Adam-mark, 2005; Casmir, 2005; North 2010; Khan 2011).

UTM as an academic environment also deals with security problems every semesters. In this system there are several types of users. Staff has more access permission to the systems information at work place (Borreson, 2006; Aloul, 2010). Therefore, conducting a survey among staff can reflect the level of information security of them.

In this study, we use the quantitative survey for gathering the awareness of staff. For designing the effective questionnaire, we use seven metrics namely Security policy, Email and web security, Social Engineering, Backup, Physical security, Password and Security attitude. With descriptive statistical analysis of data, the level of information security awareness of staff is measured. We also applied the correlation analysis for extracting the relationship between metrics and level of security awareness. These relationships and level of awareness are useful for proposing a new information security awareness program workflow. The results of this study includes information security awareness metrics, level of information security awareness of staff, relationship of metrics and a proposed security awareness workflow. These outputs can useful in future security plans and security awareness programs.

In this chapter, an overview of research including the background of the problem, statement of the problem and objectives and significant of the study will be stated.

1.2 Background of the Problem

Everyday new incidents such as data breaches, threats, risk etc are reported and almost every time these incidents are due to human errors and lack of information security awareness. Many analysts claim that human component of any information security framework is the weakest link. Information is one of the resources that an organization is heavily dependent on. If the critical information of an organization is leaked, the organization can suffer serious consequences, e.g., in the form of loss of income, loss of customers' trust and maybe legal action etc. therefore, information should be protected and secured (Risvold, 2010; Khan 2011).

Information security awareness plays an effective role in establishing the security in the systems. It can be said one of the most important criteria for evaluation safety of the system is level of security awareness of the users and employees in the organization (Siponen, 2000; Shulaili 2010). Low level of the security awareness can be a danger vulnerability points in systems. Hence several researchers (Wilson 2003; North 2006; Yacine 2008) have proposed own techniques for measuring the security awareness of the users in their organizations (Krishna, 2010). Some of them conducted own surveys with effective questionnaire for their system and users, and others proposed techniques as research-based papers (Young, 2004; Puhakainen, 2006; Albrechtsen 2010). Here we explain briefly five research about the measuring the information security awareness.

Higher education institutions possess a vast amount of information and computing power. They also provide a relatively open access to their constituents and the public. The concerns of Information Systems (IS) Security and confidentiality in higher education are not recent. In fact, they can be traced back to the 1970s (Adam-mark, 1975). But, even today, with all the available Information Systems Security and best practices, only some of universities provide acceptable InfoSec measures and establish proper InfoSec awareness training (North 2006). According to a quantitative survey of 435 higher education institutions in the US (Updegrove 2003), only a third of the examined institutions had applied InfoSec awareness training for students and staff. In fact, most InfoSec managers pay more attention to technical aspects and solutions (such as firewalls, routers, and intrusion detection software), and ignore the socio-organizational issues such as the hazards caused by end users' lack of InfoSec awareness (Katz, 2005).

These days many intruders target the human (end-user), bypassing most security controls and using techniques such as social engineering to get what they want. Hence, awareness is becoming a key factor in an organization's ability to improve security, protect information (Navarro, 2007; Bulgurcu, 2009).

Social engineering is an underestimated security risk that is rarely addressed by companies. Security awareness training and education is the most important method of preventing social engineering attacks. It should be continuous and dynamic. Organizations can reduce the impact of social engineering attacks by implementing information security awareness program (Jason Baker, 2005).

Social Engineers are well aware that low-level employees and employees with low company morale are more susceptible to a Social Engineering attack thus they are easy targets for information revealing. But since Social Engineers can attack any employee for information, all employees should be concerned with methods of attack and be aware of who to trust when a problem occurs (Hermansson 2005) (Nelson, 2004).

Since many users do not believe that anyone would ever attack them, because they are not "rich and famous", and that hackers cannot do much damage anyway (Sasse 2001; Stewart, 2009), social engineering attacks can be highly successful. This attitude is also influenced by the fact that most users do not understand how security works. The "old" way of managing information security has led to two specific problems (Adams 1999):

- users' lack of security awareness, and
- Security departments' lack of knowledge about users, producing security mechanisms and systems that are not usable. These two factors lower users' motivation to produce secure work practices.

In addition, the user's lack of security awareness and the protective measures are not well liked, among the users, or usable. Organizations also need to establish a clear and strong policy (Terry 2005; Martin, 2006; Muda, 2010), including standards, processes and procedures to help eliminate the threat of social engineering.

A significant problem is that it is not easy to investigate people’s attitudes and behavior patterns in relation to complex technological matters such as ICT security, since there is a real risk that the respondents in a survey simply do not understand the questions put to them.

Enhancing information security does not depend on only technical solutions in a company. Based on the literature (Abawajy 2008), the first and important problem in this area can be difficulty in measuring the security awareness among staffs. In fact, the problem is in designing the best and effective questionnaire to be suitable to own companies to evaluate the level of information security awareness among staffs (Mathisen, 2004; Adam-mark, 2005).

1.3 Problem Statement

The most important problem in information security issue is level of information security awareness among staffs. Usually employees don’t have enough attention about information security to protect their information system completely. The main problem is:

“The awareness, attitudes, and behavior of the users are important to make higher level of safety in our system, but for designing the new security awareness program, we need the level of current security awareness of staffs which is unfortunately not easily sensible. Hence the main problem is: “what is the level of information security awareness among employees?”

Extracted sub-questions are also as follow:

- RQ1: What are the set of metrics for measuring the level of information security awareness?
- RQ2: What is the level of information security awareness among staffs?
- RQ3: Are there significant relationships between information security awareness metrics, level of security awareness, and personal profile of staffs?

1.4 Objectives

The aims of this study are:

- To find the information security awareness measuring metrics in order to design an effective survey questionnaire
- To measure the level of information security awareness of staffs by descriptive statistical analysis tools
- To identify impact of each metrics on level of security awareness by correlation analysis

1.5 Purpose of the Study

The purpose of this study is measuring the level of information security awareness among CICT staffs. This level of awareness and also correlation analysis of metrics will be applied to propose the Critical Success Factors and effective security model.

1.6 Significance of the Study

According to the interview session with the dean of the CICT there is no information security awareness survey was conducted before. This study is an original study that can help the information security management to know what the level of security awareness among staffs is. It hopes that the result of this research offers a positive impact on the CICT organization. The result of this study can be useful in future security planning and security awareness programs.

1.7 Scope of the Study

- Respondent: All CICT staffs
- Questionnaire: based on information security awareness metrics
- Data gathering: Quantitative methodology
- Data analysis: SPSS software
- Measuring the level of awareness: Descriptive Statistical analysis
- Correlation analysis: Spearman Correlation Analysis

1.8 Summary

This chapter discussed an overview of this study. There are four project objectives that need to successfully achieve as the goals of this research. The scope and importance of this project have also been pointed out.

REFERENCES

Abawajy, J. H., K. Thatcher, et al. (2008). Investigation of Stakeholders Commitment to Information Security Awareness Programs. *Information Security and Assurance, 2008. ISA 2008. International Conference on*.

Adam-mark (2005) "*The Effect of a University Information Security Survey on Instructing Methods in Information Security*."

Adam-mark, B. K. (1975). "Security and Confidentiality in a university computer network."

Adams, A. and M. A. Sasse (1999). "Users are not the enemy." *Commun. ACM* 42(12): 40-46.

Albrechtsen, E. and J. Hovden (2010). "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study." *Computers &amp; Security* **29**(4): 432-445.

Aloul, F. (2010). "The Need for Effective Information Security Awareness." *International Journal of Intelligent Computing Research (IJICR)* Volume 1, Issue 3.

Bonoma, T. V. (1985). "Case Research in Marketing: Opportunities, Problems,

and a Process." *Journal of Marketing research* pp. 199-208.

Borreson, J. (2006) "*Safeguarding the tower: IT security in higher education*."

Bourner, T. (1996) "*The research process: four steps to success*." Research methods: guidance for postgraduates.

Bulgurcu, B. (2009). Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance. *Americas Conference on Information Systems (AMCIS).*

Casmir, R.,(2005) Casmir, R., *A Dynamic and Adaptive Information Security Awareness (DAISA) Approach*,Department of Computer and Systems Sciences, Chandler, D. (2004) "*Reviewing the Literature*." The Media and Communication Studies Site.

CIT-AWARE,(2006) CIT-AWARE, *An Investigation of Citizen ICT Safety and Security Awareness,*

Cooper, D. R. and P. S. Schindler (2003). *Business Research Method,* Brent Gordon: McGraw Hill.

Danchev, D. (2003) "*Building and Implementing a Successful Information Security Policy*." Windows Security.

Eric, L., C. Tubb, et al. (2010) "*Using Deception for Assuring Security*."

Gartner (2005) "*Management Update: How Businesses Can Defend against Social Engineering Attacks*."

Global, S. (2008) "*Information Security Awareness Survey*."

Gollmann, D. (1999). *Computer security*, John Wiley \\& Sons, Inc.

GoogleScholar. "*GoogleScholar*." from http://scholar.google.com/-.

Granger, S. (2002). "Social Engineering Fundamentals, Part II : Combat Strategies."

Gupta, V., S. Goswami, et al. (2004). "Networking and Security Measures." *DESIDOC Bulletin of Information Technology* Vol. 24, **No. 2,**.

Hair, J. F. (2005) "*Multivariate data analysis*." Pearson Prentice Hall.

Halim (2009) "*Academic Report Writing*."

Hasan, M. (2010). "Case Study On Social Engineering Techniques For Persuasion." *International journal on applications of graph theory in wireless ad hoc networks and sensor networks* 17-23.

Heare, S. (2001) "*Data Center Physical Security Checklist*."

Hermansson, M. and R. Ravne,(2005) Hermansson, M. and R. Ravne, *Fighting Social Engineering*,University of Stockholm / Royal Institute of Technology

HoneyTech (2010). *Security Awareness Survey Description*.

HoneyTech (2010) "*Security Awareness Survey Description*." Creative Commons Attribution-Noncommercial.

Huang, C.-Y., S.-P. Ma, et al. (2011). "Using one-time passwords to prevent password phishing attacks." *Journal of Network and Computer Applications* 34(4): 1292-1301.

IEEE. "*IEEE Xplore*." from http://ieeexplore.ieee.org/

Jan Møller Jensen, T. H. (2006). "An empirical examination of brand loyalty." *Journal of Product & Brand Management* Vol. 15 Iss: 7, pp.442 - 449.

Jason Baker, B. L. (2005) "*The Impact of Social Engineering Attacks on Organizations A differentiated Study*."

K Rudolph and a. L. N. Gale Warshawsky (2001). *Computer security Handbook*.

Kark, K. (2006). "Five Steps to Effective Security Awareness." *Forrester Research*.

Katz, F. H. (2005). The effect of a university information security survey on instruction methods in information security. *Proceedings of the 2nd annual conference on Information security curriculum development*, Kennesaw, Georgia, ACM.

Khan, B., K. S. Alghathbar, et al. (2011). *Information Security Awareness Campaign: An Alternate Approach Information Security and Assurance*. T.-h. Kim, H. Adeli, R. J. Robles and M. Balitanas, Springer Berlin Heidelberg. 200: 1-10.

Krishna, M.,(2010) Krishna, M., *A Methodology for Measuring Information Security Maturity in Norwegian and Indian MSME's with special focus on people factor,*

Kruger, H. A., S. Flowerday, et al. (2011). An assessment of the role of cultural factors in information security awareness. *Information Security South Africa (ISSA), 2011*.

Kruger, H. A. and W. D. Kearney (2006). "A prototype for assessing information security awareness." *Computers &amp; Security* 25(4): 289-296.

Lincoln and G. E. (1985) "*Naturalist Inquiry*." Sage Publications.

Luker, M. and R. Petersen (2003). *Computer and Network Security in Higher Education (ID: PUB7008)*, EDUCAUSE

MAAWG (2010). *Email Security Awareness and Usage Report*.

Malcolm and Allen (2007) "*Social Engineering: A Means To Violate A Computer System*."

Marks, A. and Y. Rezgui (2009). A Comparative Study of Information Security Awareness in Higher Education Based on the Concept of Design Theorizing. *Management and Service Science, 2009. MASS '09. International Conference on*.

Martin, A. P. (2006). Information Availability and Security Policy. *Proceedings of the Twelfth Americas Conference on Information Systems*.

Mathisen, J.,(2004) Mathisen, J., *Measuring Information Security Awareness – A survey showing the Norwegian way to do it,* Mathisen, J.,(2004) Mathisen, J., *Measuring Information Security Awareness – A survey showing the Norwegian way to do it*,NISlab,

McDowell, M. (2007) "*Avoiding Social Engineering and Phishing Attacks*."

MicrosoftWebpage.

Mitnick, Kevin, et al. (2002). *The Art of Deception* Wiley.

Muda, M. Z. B.,(2010) Muda, M. Z. B., *Awareness And Acceptance Analysis Of Information Security Policy*,UTM Master Thesis,

Murphy (1996) " *Backup strategy*."

Navarro, L., (2007), *Train employees - your best defense - for security awareness*

Nelson, R. (2004) "*Methods of hacking: Social Engineering*."

Nohlberg, M.,(2008) Nohlberg, M., *Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks,*

North, M., DeAnthony Perryman, et al. (2010). "A Comparative Study Of Information Security And Ethics Awareness In Diverse University Environments." *Consortium for Computing Sciences in Colleges*.

North, M. M., R. George, et al. (2006). Computer security and ethics awareness in university environments: a challenge for management of information systems. *Proceedings of the 44th annual Southeast regional conference*, Melbourne, Florida, ACM.

Parrish (2001) "*Security considerations for enterprise level backups*."

Peltier, T. R. (2005). "Implementing an Information Security Awareness Program." *Security Management Practices*.

Pfleeger, C. P. and S. L. Pfleeger (2009). *Security in Computing, 4th Edition*

PSZ. "*Perpustakaan Sultanah Zanariah* ", from http://www.utm.my/psz/.

Puhakainen, P. (2006). "A Design Theory For Information Security Awareness."

Rasli, A. (2006). *Data Analysis and interpretation*, UTM.

Riley, S., Ed.117ds. (2006). *Password Security: What Users Know and What They Actually Do*.

Risvold, M. O.,(2010) Risvold, M. O., *Organizational Issue related to information security behavior*,Lulea University of technology

Salem, O., A. Hossain, et al. (2010). Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks. *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*.

Sasse, M. A., S. Brostoff, et al. (2001). "Transforming the ‘Weakest Link’ — a Human/Computer Interaction Approach to Usable and Effective Security." *BT Technology Journal* 19(3): 122-131.

ScienceDirect. "*ScienceDirect*." from http://www.sciencedirect.com/.

Seppo, P., S. Mikko, et al. (2007). Employees' Behavior towards IS Security Policy Compliance. *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*.

Shaikh, A. A.,(2006) Shaikh, A. A., *An Investigation into the Corporate Security Awareness and Training Program*,Master’s Thesis in Accounting HANKEN-Swedish School of Economics and Business Administration

Shaw, R. S., C. C. Chen, et al. (2009). "The impact of information richness on information security awareness training effectiveness." *Computers &amp; Education* **52**(1): 92-100.

Shulaili, T., N. L. Clarke, et al. (2010). An Analysis of Information Security Awareness within Home and Work Environments. *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*.

Siponen, M., S. Pahnila, et al. (2007). *Employees’ Adherence to Information Security Policies: An Empirical Study New Approaches for Security, Privacy and Trust in Complex Environments*. H. Venter, M. Eloff, L. Labuschagne, J. Eloff and R. von Solms, Springer Boston. 232**:** 133-144.

Siponen, M. T. (2000). "A conceptual foundation for organizational information security awareness." *Information Management & Computer Security* Vol. 8 Iss: 1, pp.31 - 41.

Stewart, G.,(2009) Stewart, G., *Maximising the Effectiveness of Information Security Awareness Using Marketing and Psychology Principles,*

Terry and W. (2005). "Information security policy's impact on reporting security incidents." *Computers &amp; Security* 24(6): 448-459.

Thanasegaran, G. (2009). "Reliability and Validity Issues in Research." *Integration & Dissemination* vol. 4, pp. 35-40.

Updegrove and a. W. Gordon (2003) "*Computers and Network Security in Higher Education*." EDUCAUSE.

WIKIPEDIA. "*WIKIPEDIA*." from http://en.wikipedia.org/wiki/Spearman's_rank_correlation_coefficient

Wilson, Mark (Ed), et al. (1998). "Information Technology Security Training Requirements: A Role- and Performance-Based Model." *NIST Special Publication 800-16*.

Wilson, M. and Joan Hash (NIST) (2003) "*Building an Information Technology Security Awareness and Training Program.* ." NIST Special Publication 800-50, October 2003.

Yacine, Rezgui, et al. (2008). "Information security awareness in higher education: An exploratory study." *Computers &amp; Security* **27**(7-8): 241-253.

Young, E. a. (2004). "Global Information Security Survey."