EVALUATION OF USER'S BEHAVIORS IN HANDLING COMPUTER SECURITY INCIDENT IN FINANCIAL INSTITUTION IN KLANG VALLEY

NOR HIDAYAH BINTI MOHD JAWAWI

UNIVERSITI TEKNOLOGI MALAYSIA

EVALUATION OF USER'S BEHAVIORS IN HANDLING COMPUTER SECURITY INCIDENT IN FINANCIAL INSTITUTION IN KLANG VALLEY

NOR HIDAYAH BINTI MOHD JAWAWI

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

Advanced Informatics School (AIS)
Faculty of Computer Science and Information System (FSKSM)
Universiti Teknologi Malaysia

AUGUST 2012

Dedicated to my beloved husband and parents.

ACKNOWLEDGEMENTS

In the name of Allah, the Merciful, the Compassionate. We glorify Allah and ask blessings and send salutation upon the noble Prophet, upon his descendents, upon his companion, and upon his followers in upholding the cause of the right religion. First and foremost, I'm thankful to Allah S.W.T that through His blessing and guidance I'm able to accomplish my Project 1 entitled Evaluating Users' Behavior in Handling Computer Security Incident in Financial Institution.

Thus, I have many people to thanks for their effort in helping me to write this report completely. First, I owe special thanks for my supervisor, Prof. Dr. Zuraini Ismail. Without her help and though, I'm not be able to complete my task and submit it on the date. Thanks again for her willing and afford to spend her time in helping during the conducting the research.

Besides that, I would like to say big thanks to all who contribute in this project especially to all lecturers and my course mates that always be with me and supporting behind. Not forgotten to all my friends for their patience in allowing me the time and space to complete this project.

Finally, specials thanks for my beloved husband and parents for their support and also to others who graciously gave permission to use or cite their material, thank you so much. Thanks again to all of you for your cooperation and may Allah bless you all for your commendable contributories.

ABSTRACT

Computer security incident is any activities or events that potentially harm the computer systems or networks. These activities could be due to various vulnerabilities and threats either intentionally or unintentionally attempted such as unauthorized actions in a computer system, hardware or software failure, denial of service attempts and other events that could be threatens the computer system. As computer security incident cannot fully avoided or mitigated, organizations should have a procedure in handling such incidents to mitigate the incident, control the situation during the incident or recover the system affected by the incident. This study has been conducted to identify the components of user's behaviors in handling computer security incident. Here we found six components of user's behaviors in handling computer security incident which are aware of assurance, responsibility, perceived skills and knowledge, general security orientation, motivation and perceived barriers. An analysis of these behaviors has been done which covered the 13 financial institutions in Klang Valley. The result of analysis shows more than half of users are agree with all these components of users' behaviors in handling computer security incident except for perceived skills and knowledge. The study shown that most of users are concern with the common information security practices and sharing the detected problem with others by seeking assistance with other colleagues. However, the users are not really care with the security practices in handling computer security incident which need their effort technically. Therefore, the organizations need to note this issue to find appropriate solution

ABSTRAK

Insiden keselamatan komputer adalah suatu aktiviti atau perbuatan yang berpotensi mengganggu dan merosakkan sistem komputer atau rangkaian. Aktiviti-aktiviti ini boleh disebabkan oleh pelbagai faktor sama ada secara sengaja atau tidak seperti pencerobohan sistem komputer tanpa kebenaran, kegagalan perkakas komputer atau perisian burfungsi, dan sebagainya yg boleh mengancam sistem komputer. Oleh kerana insiden keselamatan komputer tidak dapat dielakkan sepenuhnya, setiap organisasi perlu mempunyai langkah-langkah dalam mengendalikan insiden yang berlaku sama ada untuk memberhentikan insiden tersebut, mengawal keadaan semasa insiden belaku bagi memastikan sistem masih berfungsi atau membaiki sistem yang terjejas disebabkan insiden yag berlaku. Kajian ini mengenalpasti perangai pengguna dalam mengendalikan insiden keselamatan komputer and mengkaji langkah-langkah pengguna di syarikat-syarikat kewangan di Malaysia semasa menghadapi insiden keselamatan komputer. Kajian dapat mengenalpasti enam komponen perangai pengguna dalam mengendalikan insiden keselamatan konputer iaitu kesedaran terhadap jaminan, tanggungjawab, kemahiran dan pengetahuan, pengetahuan umum tenteng keselamatan, motivasi dan halangan. Kajian terhadap komponen-komponen ini telah dijalankan di 13 syarikat kewangan di kawasan Lembah Klang melalui kaedah kaji selidik. Keputusan kajian mendapati kebanyakan pengguna bersetuju dengan komponen-komponen ini kecuali kemahiran dan pengetahuan. Selain itu, kajian mendapati kebanyakan pengguna mengambil berat tentang asas amalan keselamatan dan akan berkongsi masalah keselamatan yang dihadapi bersama rakan sekerja. Tetapi, mereka kurang mengambil berat tentang amalan keselamatn komputer yang memerlukan kemahiran teknikal. Oleh itu, langkah-langkah penyelesaian perlu diambil untuk mengatasi masalah ini.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CSIRT	-	Computer Security Incident Response Team
CIO	-	Chief Information Officer
CISO	-	Chief Information Security Officer
CEO	-	Chief Executive Officer
CERT	-	Computer Emergency Response Team
IT	-	Information Technology
IRP	-	Incident Response Plan
IR	-	Incident Response
PC	-	Personal Computer

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Computer security incidents are any activities or events that potentially harm the computer systems or networks. These activities could happen due to the various vulnerabilities and threats either intentionally or unintentionally attempted such as unauthorized actions in a computer system, hardware or software failure, denial of service attempts and other events that could threaten the computer system.

As reported by MyCERT, Cybersecurity Malaysia, the computer incidents in Malaysia is increasing from year to year. Figure 1.1 shows the statistic of the reported incidents from 2007 until 2011.

Based on the statistic in Figure 1.1, the number of computer incidents are slightly increased from 2007 until 2009. After that, it was drastically increased until 2011. It shows that computer incidents will be critical issues in the future if they are not being handled and managed properly.

Once these incidents cannot be controlled, it may harm the computer system and disrupt the business operation. Hence, it will affect the revenue of the businesses.

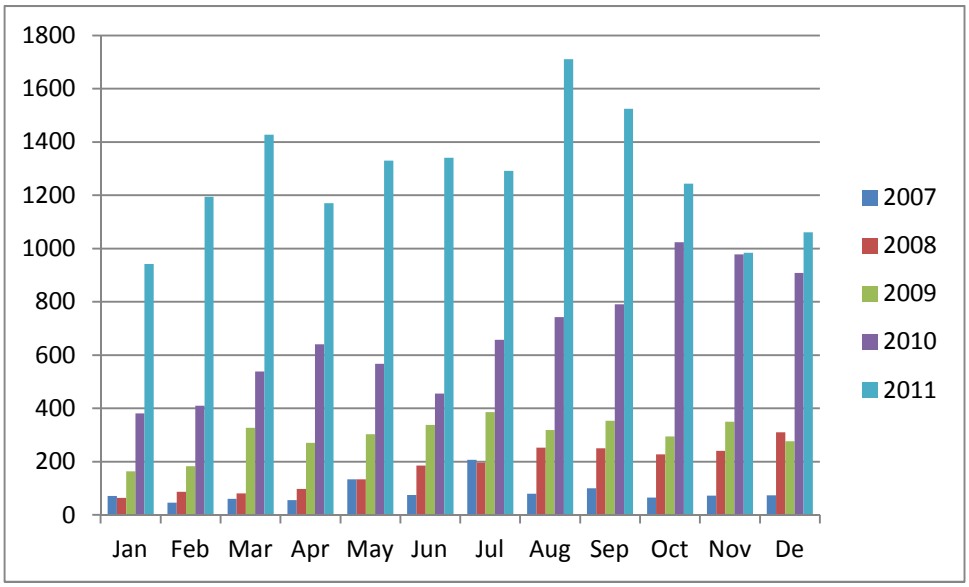

Figure 1.1: Comparison of the reported incidents from 2007 until 2011

An incident might cause a billion of revenue lost in an organization. Therefore, each organization including financial institution should have their own Computer Security Incident Response Team (CSIRT) to manage and handle these incidents in order to ensure the continuity of their business.

However, this research is not a study on how to manage the CSIRT but to look into users' behaviors in handling the computer security incidents. It includes the actions taken by users when facing computer security incidents.

This research focuses on financial institutions including banking and insurance companies in Malaysia since we believe that these organizations are the most attractive targets for attackers to launch their attack.

1.2 Background of the Problem

Nowadays, most of the organizations realize the importance of the incident management and set up their own CSIRT to manage any potential incident that might harm their operation. The CSIRT is responsible to provide the incident response plan to control the business operation when an incident happens .It is also to prevent any loss or damage.

Within a single organization with an incident response plan, the response will generally be controlled through a single entity such as an incident response team where the team will report to a single individual, such as the Chief Information Officer (CIO), Chief Information Security Officer (CISO), or Chief Executive Officer (CEO) for industry organizations (White, G. Granado, N, 2009).

However, not all of the users are aware with the existence of the security team in their organization. Rheea H. S. *et al*., (2009) suggested that no matter how effective the technical layer of security is being provided, the security posture ultimately depends on appropriate end user behavior. Behavior is the range of actions and mannerisms made by organisms, systems, or artificial entities in conjunction with their environment, which includes the other systems or organisms around as well as the physical environment. Hence, user behavior is the way in which one acts or conducts oneself towards others. However, this study only looks into the way of people act or conducts the computer security incident.

No matter how much policies are produced, how effective the procedures are developed, it will depend on the users' behavior in sense of how far they understand the policies or procedure, and their ability to apply them in daily tasks. Therefore, this research is conducted to see users' behaviors in handling the computer security incidents.

1.3 Problem Statement

The need of CSIRT today is very important in an organization especially in financial institution because of the confidential and valuable information. In relation to that, financial institutions face a wide range of highly motivated and active threat sources (Bonnette C.A., 2003). As current report shown in Symantec.com, 16% of the data breach was reported from the financial institution including insurance sectors which is the third most likely category of organization to be attacked. Then, these data breach could lead to identity theft and it was reported that 29% of identity theft occurred in financial institution including insurance company. It is noted that financial institutions are the most likely category of organization to be attacked in identity theft. Since financial institutions are a main target of attackers, they might be facing with various types of computer incidents.

In order to ensure the incidents do not disrupt the business operation, the CSIRT should apply incident handling process. However, this process presents a number of challenges as financial institutions have their unique circumstances which drive overall risk in its operations which is based on the sensitivity of the information and different view of management to classify the severity and danger of the incidents. Therefore, different organization will have different procedure in handling incidents. Hence, security professionals who are in charge in protecting their organizations' information assets must understand the source of these attacks, along with their likelihood of occurrence and related impact (Bonnette C.A., 2003). Besides that, users also should understand and able to manage computer incidents that might be happen to ensure the effectiveness of handling the incidents.

1.4 Project Objectives

The objectives of this research are as below:

1. To identify the components of users' behaviors in handling computer security incidents.
2. To propose a model of users' behaviors in handling computer security incidents.
3. To evaluate the users' behaviors in handling computer security incidents in financial institution in Malaysia.

1.5 Research Question

This research will answer the following questions:

1. What are the components of users' behaviors in handling computer security incidents?
2. How did the components of users' behaviors worked in handling computer security incidents?
3. How effective is the users' behaviors in handling computer security incident in financial institutions?

1.6 Project Aim

The aim of this research is to identify the components of users' behaviors in handling computer security incidents and to analyze on how it works by proposing a

model in order to measure the effectiveness of the users' behaviors in handling computer incidents in financial institutions.

1.7 Project Scope

This research concerns on below circumstances:

1. The research will focus on employee working in financial institution in Malaysia where the companies are located in Klang Valley. We only look at users' behaviors in handling computer security incidents. The users will be selected randomly from IT and non IT background.
2. This research will be conducted by using quantitative method where questionnaire will be used as a survey instrument. The data collected from the questionnaire will be interpreted and presented in Microsoft Office Excel 2007. Then, the data will be analyzed by using statistical method. The result of analysis will be presented in chart and graph.

1.8 Summary

This chapter presents the idea of this research. The introduction and overview of this research is briefly explained. The project objectives are defined and the project's aim is clearly stated to ensure this research meets what it is looking for. Besides that, the research questions and the project scope are also being specified to ensure that it will achieve the objectives of this research.

REFERENCES

Albrechtsen E., Hovden J. (2009). *Improving Information Security Awareness and Behaviour Through Dialogue, Participation And Collective Reflection. An Intervention Study*. Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology, N-7491 Trondheim, Norway

Beaupre A. (2009). *Incident Response vs. Incident Handling* retrieved on May 3, 2012 from https://isc.sans.edu/diary/Incident+Response+vs+Incident+Handling/6205

Bejtlich, R. (2005). *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. Boston, MA: Pearson Education, Inc.

Bonnette C. A. (2003). *Assessing Threats to Information Security in Financial Institutions*. GSEC Certification Practical Assignment,Version 1.4b - Option 1. ht

BusinessDictionary.com retrieved on October 13, 2011 from http://www.businessdictionary.com/definition/financial-institution.html

ENISA's Good Practice Guide on Incident Reporting Mechanisms retrieved on December 02, 2011 from http://www.enisa.europa.eu/.../good-practices.../incident-reporting-mechanism.Expatriate Malaysia Insurance Guide - Life and General Insurance Companies in Malaysia retrieved on December 20, 2011 from http://www.expat.com.my/Expatriates%20Malaysia%20Guide%20-%20Insurance%20Companies%20in%20Malaysia.htm

Fiza binti Abdul Rahim (2009). *Comprehensive Analysis on The Influences Of Computer Ethics On Information Security.* Centre for Advanced Software Engineering (CASE), Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia

Grance T., Kent K., Kim B. (2004). *Computer Security Incident Handling Guide*. National Institute of Standards and Technology.

Haniza binti Sharif (2009). *Users' Perception of The Information Security Policy At Universiti Teknologi Malaysia.* Centre for Advanced Software Engineering Faculty of Computer Science and Information Systems Universiti Teknologi Malaysia.

Kumar and Ranjit (2005) Research Methodology-A Step-by-Step Guide for Beginners,(2nd.ed.),Singapore, Pearson Education.

M. E. Kabay (2009), *CSIRT Management*. School of Business & Management Norwich University

Melissa Guenther (2001). *Security Awareness Quiz Questions*. LLC. All rights reserved.

Mitropoulos S., Patsos D., Douligeris C. (2005). *On Incident Handling and Response:A state-of-the-art approach*. Department of Informatics, University of Piraeus, 80, Karaoli and Dimitriou Street,Piraeus 185 34, Greece

MyCERT Incident Statistic retrieved on October 13, 2011 from http://www.mycert.org.my/en/services/statistic/mycert/2011/main/detail/795/index.html

Ng B. Y., Kankanhalli A, Xu Y. (2008). *Studying Users' Computer Security Behavior: A Health Belief Perspective*. Department of Information Systems, National University of Singapore, Singapore

Patrick K., (2011).*The Incident Handlers Handbook*. GIAC (GCIH) Gold Certification

Patsos D. A (2002). *Strategic Approach to Incident Response*. Department of Mathematics/Information SecurityGroup, Royal Holloway University of London

Rheea H. S., Kimb C., Ryuc Y. U.(2009). *Self-Efficacy In Information Security: Its Influence On End Users' Information Security Practice Behavior.* Asian and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT), USA

Scarfone K., Grance T., Masone K.(2008) . Computer Security Incident Handling Guide: *Recommendations of the National Institute of Standards and Technology* (MD 20899-8930), National Institute of Standards and Technology Gaithersburg

Site Security Review retrieved on December 02, 2011 from *https://www.gridpp.ac.uk/security/document/Site_Security_Review.pdf.*

Stanton J. M., Stam K. R., Mastrangelo P., Jolton J. (2004). *Analysis of End User Security Behaviors*. Center for Science and Technology, School of Information Studies, Syracuse University,Syracuse, NY 13244-4100, United States

Threat Activity Trends retrieved on December 20, 2011 from http://www.symantec.com/business/threatreport/topic.jsp?id=threat_activity_trends&aid=data_breaches

White, G. Granado, N. (2009). *Developing a Community Cyber Security Incident Response Capability*. Proceedings of the 42nd Hawaii International Conference on System Sciences: IEEE, 978-0-7695-3450-3/09

Whitman M.E, Mattord H. J. (2008). *Management of Information Security.* (2nd ed.) Kennewas State University: Course Technology Cengage Learning.