COMPREHENSIVE ANALYSIS ON THE INFLUENCES OF COMPUTER ETHICS ON INFORMATION SECURITY

FIZA ABDUL RAHIM

UNIVERSITI TEKNOLOGI MALAYSIA

COMPREHENSIVE ANALYSIS ON THE INFLUENCES OF COMPUTER ETHICS ON INFORMATION SECURITY

FIZA BINTI ABDUL RAHIM

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

APRIL 2009

ACKNOWLEDGEMENT

The highest gratitude to Allah the Almighty as of with his blessings and permission I have, alas, been able to complete this project report for my Master Degree.

I would like to take this opportunity to present my deepest gratitude to my project supervisor, Dr. Zuraini binti Ismail for her encouragement and guidance. Special thanks to all lecturers and staffs at Centre for Advanced Software Engineering (CASE) for their cooperation and support throughout my course at CASE.

I am also very thankful to my husband En. Mohd. Al-Hafiz Ahmad for his everlasting support in all terms since I started this project. A million thanks to my family and friends too who always encouraged me and gave me full support to finish this project. Thank you.

ABSTRACT

Many ethical issues related to computer remains to be a concern regardless the mode of activity. Computer security, therefore, must also be concerned with the actions of trusted computer users. Since businesses have increased their usage of computers, an organization must play a major role in developing ethical awareness among employees so that they will make ethical choices regarding computer activities while in workplace. Therefore, the purposes of this project are to identify which component of computer ethics influence information security, to develop framework of computer ethics and information security and to determine the relationship between computer ethics and information security. Several statistical methods are used throughout the analysis. This project is expected provide an exposure on the importance of computer ethics and information security in an organization. Solutions need to be taken to deal with potential of unethical behavior associated with the use of information.

ABSTRAK

Terdapat pelbagai isu etika yang berkaitan dengan penggunaan komputer yang masih menjadi satu kebimbangan dalam apa jua mod aktiviti. Isu keselamatan komputer juga penting kerana kebarangkalian jenayah dilakukan oleh pengguna komputer yang dipercayai. Sejak perniagaan dan organisasi meningkatkan penggunaan komputer dalam urusan kerja seharian, organisasi perlu memainkan peranan dalam meningkatkan kesedaran etika di kalangan pekerja-pekerja supaya mereka akan membuat pilihan yang beretika mengenai aktiviti-aktiviti komputer yang dijalankan di tempat kerja. Oleh itu, tujuan projek ini adalah untuk mengenalpasti komponen etika komputer yang mana dapat mempengaruhi keselamatan maklumat, untuk membangunkan rangkakerja bagi etika komputer dan keselamatan maklumat dan untuk menentukan hubungan antara etika komputer dan keselamatan maklumat. Beberapa kaedah statistik digunakan sepanjang analisis. Adalah diharapkan agar projek ini dapat memberi pendedahan terhadap kepentingan etika komputer dan keselamatan maklumat di dalam organisasi. Penyelesaian perlu diambil untuk berurusan dengan potensi tingkah laku tidak beretika yang berkaitan dengan penggunaan maklumat.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AASU	-	Armstrong Atlantic State University
CASE	-	Centre for Advance Software Engineering
CE	-	Computer Ethics
CEI	-	Computer Ethics Institute
CST	-	College of Science and Technology
e-Government	-	electronic-Government
ICT	-	Information and Communication Technology
IS	-	Information Security
IT	-	Information Technology
KMO	-	Kaiser-Meyer-Olkin
US	-	United States
UTM	-	University Technology Malaysia
VS	-	Versus
WWW	-	World Wide Web

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Computer usage has increasingly become a part of human's life because it provides us with many capabilities and these in turn give us new choices for action. Realizing its impertinent presence, the Malaysia government has shown its commitment in the use of information and communication technology (ICT) with the implementation of electronic-Government (e-Government). Thus signified Malaysia's effort in transforming the way it operates, modernizing and enhancing its service delivery.

Computer files, databases, networking and the Internet-based applications all have gradually become part of the most critical assets of an individual and organization. When these assets are attacked, damaged or threatened, data integrity becomes an issue and the proper operation of the business may be interrupted. Therefore, the need of computer ethics is crucial and the use of computer technology should be controlled, monitored and guided to protect users and organizations from computer threats.

The misuse of computers and unethical behaviour related to computer application systems has resulted in serious losses to business and society. As never before, computer-based technology provides organizations the opportunity to have

almost instantaneous access to vast amounts of critical information about customers, competitors, employees, and suppliers.

Organizations are commonly affected by incidents such as information violations, misuse of peer file sharing and accessing inappropriate websites. Hence, this project will examine computer ethics and computer security among employees of Klang Valley organizations. Finally, the study will describe the relationship between computer ethics in the world of information security, and which component of computer ethics influences information security.

1.2 Background of the Study

Computers can perform almost any task and obviously pose a threat to jobs. At the same time, computers are often far more efficient than humans in performing many tasks. Therefore, economic incentives to replace humans with computerized devices are very high. Indeed, in the industrialized world many workers already have been replaced by computerized devices, for example, bank tellers, auto workers, telephone operators, typists, graphic artists, security guards, assembly-line workers, and many others. In addition, even professionals like medical doctors, lawyers, teachers, accountants and psychologists are finding that computers can perform many of their traditional professional duties quite effectively.

In this era of computer “viruses” and international spying by “hackers” who are thousands of miles away, it is pertinent that computer security is a topic of concern in the field of computer ethics. Malicious kinds of software, or “programmed threats”, provide a significant challenge to computer security. These include “viruses”, which cannot run on their own, but rather are inserted into other computer programs; “worms” which can move from machine to machine across networks, and may have parts of themselves running on different machines; “Trojan horses” which appear to be one sort of program, but actually are doing damage behind the scenes; “logic bombs” which check for particular conditions and then

execute when those conditions arise; and “bacteria” or “rabbits” which multiply rapidly and fill up the computer's memory.

Computer crimes, such as misuse or planting of logic bombs, are normally committed by trusted personnel who have permission to use the computer system. Computer security, therefore, must also be concerned with the actions of trusted computer users.

The ease and efficiency with which computers and computer networks can be used to gather, store, search, compare, retrieve and share personal information make computer technology especially threatening to anyone who wishes to keep various kinds of sensitive information (e.g., medical records) out of the public domain or out of the hands of those who are perceived as potential threats. One of the more controversial areas of computer ethics concerns the intellectual property rights connected with software ownership. The software industry lost almost millions of dollars in sales because of copying. Ownership is a complex matter, since there are several different aspects of software that can be owned and three different types of ownership: copyrights, trade secrets, and patents.

Many ethical issues related to computer use are issues that are concern regardless of the mode of activity. Businesses have struggled for many years with people who take credit for someone else’s work. The availability of wide-ranging sources of information on the Internet has made it much easier to obtain someone else’s work than was previously.

1.3 Problem Statement

Computer-based technology provides organizations the opportunity to have almost instantaneous access to vast amounts if critical information about customers, competitors, employees and suppliers. Since businesses have increased their usage of computers, an organization must play a major role in developing ethical

awareness among employees so that they will make ethical choices regarding computer activities while in workplace.

Incidents involving privacy violations, data theft and many more have emphasized the potential of unethical behavior associated with the use of information, and there is the importance of information security due to the increased utilization of computers and Internet. It is necessary to study the relationship between computer ethics and information security and how does computer ethics influence information security.

1.4 Objectives

The objectives of this project will be as follows:

- To identify which component of computer ethics influence information security.
- To develop framework of computer ethics and information security.
- To determine the relationship between computer ethics and information security.

1.5 Scope of Research

This project will focus on determining the relationship between computer ethics and information security. There were two scopes have been identified to facilitate research understanding and management;

- Research site scope concentrated among employees in Klang Valley which are working in manufacturing and services industry in two types of organization, government and private sector.

- Data was collected from respondents using questionnaire were gathered from a stratified random sample using the local online search directory (http://www.701panduan.com/) and Malaysia's Government Official Portal (http://www.gov.my/).

1.6 Project Requirement

For the purpose of completing this study, the following equipments are required:

(a) Hardware Requirements

In order to ensure the actual requirements needed, comparison and observation have been done. Below are the components of hardware requirement that were used:

(i) Personal Computer with 1.8 GHz Pentium IV CPU;
(ii) At least 512 Megabytes of RAM;
(iii) 20 Gigabyte Hard Drive;
(iv) USB Ports; and
(v) Printer.

(b) Software Requirements

During the level of choosing the appropriate software to facilitate in doing this research, detail observation should be emphasized. From the observation that have been done, the software that being used are:

(i) Operating System: Microsoft XP;

(ii) Office Application: Microsoft Office XP, Microsoft Project, Microsoft Visio; and

(iii) Statistical software – To perform data analysis including solutions for Data Integration and Analytics, SPSS version 15.0 & 17.0.

(c) Questionnaire

One primary survey method is used to elicit information from respondents, Questionnaire. The questionnaire for this research can be referred in Appendix A.

1.7 Summary

This chapter begins with the overview of this computer usage, computer ethics and information security along with the background of the study, problem statement, research objectives, scope of research and project requirement.

REFERENCES

Argandoña, A. (2003). "On ethical, social and environmental management systems," IESE Research Papers D/508, IESE Business School.

Bailey. D. (2008). *Cyber Ethics*. Rosen Central.

Baker, T. L.. (1994). *Doing Social Research.* 2nd Edition. Singapore: McGraw-Hill Book Co. 171-206.

Brey, Philip. (2000). "Method in Computer Ethics: Toward a Multi-Level Interdisciplinary Approach," *Ethics and Information Technology*, Vol. 2, No. 2, pp. 125-129.

Bynum. T. W. (2001). Computer and Information Ethics: Basic Concepts and Historical Overview, Stanford Encyclopedia of Philosophy.

Bynum, T. W. and Rogerson, S. (1998). "Introduction and Overview: Global Information Ethics," Science and Engineering Ethics, Vol. 2, No. 2.

Bynum T. W. and Moor J. H. eds. (1998), The Digital Phoenix: How Computers are Changing Philosophy (Oxford: Blackwell).

Cappel, J. & Windsor, C. (1998) A comparative investigation of ethical decision making: information systems professionals versus students, ACM SIGMIS Database, Volume 29, Issue 2, Page 20-32.

CEI. (1992). "Ten Commandments of Computer Ethics", Computer Ethics Institute.

Cohen, J. & Cohen, P. (1983) Multiple Regression/Correlation for the Behavioral Sciences 2nd ed. : Hillsdale, NJ: Erlbaum Associates, 67-69, 490-497.

De George, Richard T. (2003). *The Ethics of Information Technology and Business*, Blackwell Publishing.

Floridi, L. (2005). "Internet Ethics: The Constructionist Values of Homo Poieticus," in R. Cavalier (ed.), *The Impact of the Internet on our Moral Lives*, Albany: SUNY Press, 195-214.

Foltz, B. and Hauser, R. (2005). “Faculty Awareness of University Computer Usage Regulations”. 2005 Southern Association of Information Systems Conference.

Forester, T. and P. Morrison (1990). *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*, Cambridge, MA: MIT Press.

George, J. F., Batra, D., Valacich, J. S. and Hoffer, J. A. (2004). *Object-Oriented System Analysis and Design.* New Jersey: Pearson Education, Inc.

Heron, W. T., Cavico, F., Mujtaba, B. G. and Pellet, P. F. (2007). *Ethics and Information Technology Professionals: An Examination of Gender, Age, Career Stage, Education Level and Ethics Training Variables.* 2007 EABR (Business) & ETLC (Teaching) Conference Proceedings, Venice, Italy.

Johnson. D. G. (1985). *Computer Ethics.* Englewood Cliffs, New Jersey, Prentice Hall.

Johnson. D. G. (2007). Computer Professional Ethics in Theory and in Practice, 29th International Conference on Software Engineering (ICSE'07 Companion), IEEE, Computer Society.

Jones and Bartlett. (2004) Readings in Cyberethics. 2nd edition.

Jong. W.S. (2007). Information Security Component Framework and Interfaces for Implementation of SSL, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.10.

Katz, F. H. (2005). “The Effect of a University Information Security Survey on Instruction Methods in Information Security”. Information Security Curriculum Development (InfoSecCD) Conference ’05. ACM. Kennesaw, GA, USA.

Kim, J. and Mueller, C. W. (1978). Introduction to factor analysis: What it is and how to do it. Beverly Hills, CA: Sage.

Marshall. K.P. (1999). "Has technology introduced new ethical problems?", *Journal of Business Ethics*, Vol. 19 No.1, pp.81-90.

Maslin, M. and Zuraini, I. (2008). “Computer Security and Computer Ethics Awareness: A Component of Management Information System”. IEEE.

Mason, R. O. (1986). “Four Ethical Issues of the Information Age”. MIS Quarterly. Vol. 10. No.1.

Neuman, W. L. (2003). *Social Research Methods, Qualitative and Quantitative Approaches*, 5th Edition. Boston: Allyn and Bacon. 263-303.

Nunnaly, J. (1978). Psychometric theory. New York: McGraw-Hill.

North, M. M., George, R. and North, S. M.. (2006). "Computer Security and Ethics Awareness in University Environments: A Challenge for Management of Information Systems". ACM SE'06. ACM, Florida, USA.

Peltier. R. (2005). Information Security Risk Analysis, 2005, CRC Press.

Preston, D. S. and Kanagaratnam, U. D. (2000) *Ethical Issues of Telemedicine in the U.K* - ITCH 2000 from Potential to practice - International Conference, August 23-27, Victoria.

Rubin, A. And Babbie, E. R. (2008). Research Methods for Social Work. Sixth Edition. Thomson, USA.

Sani. R. (2006). "Cybercrime Gains Momentum", April 3, *New Straits Times*,

Sapiah, S. & Rose, A. A. (2006). Information Ethics in Malaysia Paperless Hospital. Proceedings of the Postgraduate Annual Research Seminar 2006: 314-318.

Siponen. T. (2001). Five Dimensions of Information Security Awareness *Computers and Society*.

Sullins, J. (2005). Ethics and artificial life: From modeling to moral agents, Ethics and Information Technology, 7:139-148.

Tavani, H and Grodzinsky, F. 2002. "Cyberstalking, Some Moral Implications", *Computers and Society*, March, 2002.Refereed**.**

Trevino, L., (1992). "Moral Reasoning and Business Ethics: Implications for Research, Education, and Management," *Journal of Business Ethics.*

Victor, B. and Cullen J. B. (1987). "Theory and Measure of Ethical Climate in Organizations." *Research in Corporate Social Performance and Policy, 9*: 51-71.

Wyld, D. C., & Jones, C. A. (1997). The importance of context: The ethical work climate constructs and models of ethical decision-making - An agenda for research. *Journal of Business Ethics, 16,* 465-472.

Yassin. Y. and Yunos. Z. (2006). "Ethics in Info Security". *NST Tech & U.* November 20, 2006, pp. 1-4.