ENHANCEMENT OF INFORMATION SECURITY MANAGEMENT SYSTEM BY EMBEDDING CORPORATE ETHICAL VIRTUE AS ETHICAL ISSUES SOLUTION

NUR ZAFIRAH BINTI ABD HASHIM

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

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2015

This project report is dedicated to my lovely husband; Muhammad Iqbal Tariq and my parents; Abd Hashim, Rohani, Idris and Norliza and to my siblings for their endless support and encouragement.

ACKNOWLEDGEMENT

First and foremost, Alhamdulillah to my creator the Almighty. I would like to express heartfelt gratitude to my supervisor Prof Madya Dr Norafida Ithnin for her constant support during my study at UTM. She inspired me greatly to work in this project. Her willingness to motivate me contributed tremendously to our project. I have learned a lot from her and I am fortunate to have her as my mentor and supervisor

I also want to express my gratitude to my husband and family members for their endless support and gave me advice when I am needed.

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I need during process.

ABSTRACT

The effectiveness and successful of the Information Security (IS) can be influences by many factors such as the human, process, technology and organizational. Hence, the Information Security Management System (ISMS) is an appropriate approach for handling and managing the information security. However, there are issues of an ethical among human and organizational cultures which affect the successful of the information security. This is because of only focusing on the technical aspect rather than human and organizational solution. The small implementing of the ethics within the information security management leads to leakage of the information in the organization. Thus, the information must be protected by highlight the important of the ethical to make the information valuable assets to the organization. Due to these issues, there are several ethical issues in information security management such as human factor as illegal behaviour and human error, the technology, the process of information security management as accountability and responsibility and also the management and organizational culture factors of information security. In this research, the PDCA is an approach used as the Information Security Management (ISM) which consist of the plan, do, check and act phase. In order to evaluate the enhancement of the ISMS process, the selected Corporate Ethical Virtue (CEV) component is embedded toward the processes as an ethical issues solution. The selected CEV components are Supportability, Clarity, Discussability, Transparency, Sanctionability, Feasibility and Congruency. The proposed of enhancement ISMS process by embedding CEV as an ethical issues solution is validate by the credibility experts.

ABSTRAK

Keberkesanan dan kejayaan di dalam keselamatan maklumat boleh dipengaruhi oleh beberapa factor seperti manusia, proses, teknologi dan organisasi. Oleh itu, Sistem Pengurusan Keselamatan Maklumat (ISMS) merupakan satu pendekatan yang sesuai untuk menangani dan menguruskan keselamatan maklumat. Walau bagaimanapun, terdapat isu-isu etika di dalam yang akan mempengaruhi manusia dan organisasi yang akan memberi kesan kepada kejayaan sesebuah keselamatan maklumat. Ini adalah kerana kebiasaan keselamatan maklumat hanya memberi tumpuan kepada aspek teknikal dan bukannya penyelesaian manusia dan organisasi. Pelaksana etika yang kurang di dalam pengurusan keselamatan maklumat membawa kepada kebocoran maklumat di dalam organisasi. Oleh itu, maklumat yang perlu dilindungi dan penting di dalam organisasi sedikit sebanyak dipengaruhi oleh etika. Oleh kerana isu-isu ini, terdapat beberapa isu-isu etika di dalam pengurusan keselamatan maklumat seperti faktor manusia sebagai perilaku tidak beretika dan kesilapan manusia, teknologi, proses pengurusan keselamatan maklumat ditafsirkan sebagai akauntabiliti dan tanggungjawab dan juga pengurusan dan budaya di dalam organisasi. Dalam kajian ini, PDCA adalah satu pendekatan yang digunakan sebagai Pengurusan Keselamatan Maklumat (ISM) yang terdiri daripada fasa-fasa merancang *(Plan*), buat (*Do*), periksa (*Check*) dan bertindak (*Act*). Dalam usaha untuk menilai peningkatan proses ISMS, komponen *Corporate Ethical Virtue* (CEV) yang dipilih untuk diterapkan di dalam proses sebagai penyelesaian kepada isu-isu beretika. Komponen (CEV) terpilih ialah *Supportability, Clarity, Discussability, Transparency, Sanctionability, Feasibility* dan *Congruency* pengurusan dan penyeliaan. Cadangan penambahbaikan proses ISMS dengan menerapkan komponen-komponen CEV sebagai isu-isu penyelesaian etika adalah disahkan oleh pakar-pakar yang berkredibiliti.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVIATIONS	DESCRIPTION
CEV	Corporate Ethical Virtue
ISM	Information Security Management
ISMS	Information Security Management System
IS	Information Security
SoA	Statement of Applicability

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, information flow in the organization may create by the employees by exchange any of related information of the organization. Hence, the security of the information is the most critical issues that need to be stress by the organization in order to exchange or sharing the information.

But, most of the solution of managing the information only based on the technical solution rather than others factor such as ethical issues as human factor towards the information security. The ethical issues may give the impact or influenced on the successful in the information security. Unfortunately, according to some researcher, lack of implementation of the ethical issues towards the information security management leads to untrusted and unsecure of the information in the organization. Thus, the information must be protected by highlight the important of the ethical to make the information valuable assets to the organization.

1.2 Problem Background

The information security management is defined as a set of policy that concern information security elements such as confidentiality, integrity and availability of the information (Kruger and Kearney, 2006). But nowadays, the lacked of securing the information is much critical because most of the process or the approaches within the information security management more focus on the technical solution.

In fact, according to CSI computer crime and security survey stated that around 52% still infected with the virus even though 98% of the user have the antivirus on the computer (Richardson, 2007). This shows that, if only the technical part is working to secure the information, the individual should take the risk of leaking the security of the information. Indeed, to mitigate this problem, the ethics elements need to be involved in the information security management system process to enhance the security of the information.

Another issue of information security in the ethical behavior is related to the right behavior. The survey was stated that 62% of the employee was monitoring others employee's email and internet usage (Electronic policies and practice survey, 2001). This shows that the lacking of the internet behavior that related in ethical issues give impact on the information and employees trusted. Besides that, based on the Information security breaches survey stated that protecting of the customer information is the most importance for security that contain of 28% while 19% of preventing outages and downtime in the Internet worm attacks (Potter & Beard, 2010)

Information security management system (ISMS) is an approach to handle the information security. However, the approach mostly used is focusing on the technical approach for example developing the policy rather than ethical solution. Thus, to minimize the issues, some solutions on the technical and ethical solution can be balance

towards to secure the information. Other than that, the research of the ethical issues in the information security is investigated the solution to enhance the information security.

The Corporate Ethical Virtue (CEV) is a measurement model of the ethical culture of the organization. The CEV is an approach of normative formulates of criteria for the ethical culture in the organizations (Muel Kaptein, 2008). Thus, in order to enhance the information security management system (ISMS) process which may help the organization to secure and manage the information as the ethical solution within in the organization among employee, customer or stakeholder.

1.3 Problem Statement

Ethical issues influence the employee's behaviors, organizational cultures and processes towards the information, customer or stakeholder as the valued assets in the organization. Others than that, ethic elements that implement will makes the information more secure in privacy of the information and benchmark to evaluate the behavior of the employee. Unfortunately, information security is more focus on the technical solution rather than ethical solutions and lacking of implementing the ethical issues in the organization leads to information's leaked. As a consequence, both organization and the employee are open to the potential threat such as privacy breach, low awareness among committees and untrusted towards the information's goal.

1.4 Project Aim

The aim of this project is to propose of embedding corporate ethical virtue in the information security management system process by using the PDCA approach as the ethical issues solution.

1.5 Objectives of the Project

There are three objectives in this project. The objectives are:

i. To study the ISMS process and CEV component in managing ethical solution in information security and analyzed current ISMS process and CEV component.
ii. To propose an ethical solution by embedding the CEV components to enhancing the ISMS process.
iii. To evaluate the enhancement of the ISMS process as an ethical issues solution by selecting CEV components in the information security.

1.6 Project Scope

The scopes of this project are:

i. This research is focus on the ISMS process as PDCA approach.
ii. This research stress on the CEV component to solved the possible ethical issues of the information security in the ISMS process.
iii. The enhancement in the ISMS process is by evaluation from the credible experts based on the distributed questionnaire.

1.7 Significant of the Project

The information security should focus not only on the technical part, but also need to focus on the human behavior or attribute to make the information more secure and effective to the organization. This is because the human factors influences in the

successfully of the information. Thus, the management and individual with high of ethics should take action to prevent breach of the information from happen.

1.8 Organization of Report

The report consists of six chapters. The description of each chapter is details in following sentences. Chapter 1 discussed about overview of the study, problem background, problem statement, aim of the project, objectives and scope. Chapter 2 consists of the literature review related in research area. The focus is on ISMS process, information security and ethical issues. Chapter 3 include of research methodology used in this project. Chapter 4 is stress on the process enhancement of the ISMS process with the selected CEV components. The analysis and result of this research is concluded in the Chapter 5. The discussion and conclusion of this project is on Chapter 6.

REFERENCES

Alavi, R., Islam, S., &Mouratidis, H. (2014).A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations.In Human Aspects of Information Security, Privacy, and Trust (pp. 297-305).Springer International Publishing.

Alfantookh, A. (2009). An Approach for the Assessment of The Application of ISO 27001 Essential Information Security Controls. *Computer Sciences, King Saud University*.

Alfantookh, A., & Bakry, S. H. (2009). IT governance practices: ITIL.*Saudi Computer Journal: Applied Computing and Informatics,7*(1), 56-65.

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Bhaskar, S. M. (2008).*Information Security: A Practical Approach*. Alpha Science International, Ltd.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104). ACM.

Broderick, J. (2006). 'ISMS, security standards and security regulations.' information security technical report 11(1).

Chang, S. E., Chen, S.-Y., and Chen, C.-Y. (2011). Exploring the Relationships between It Capabilities andInformation Security Management. *International Journal of Technology Management* (54:2/3), pp 147-166.

D'Arcy J, Hovav A &Galletta DF (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 20(1): 79–98.

DeBode, J. D., Armenakis, A. A., Feild, H. S., & Walker, A. G. (2013). Assessing Ethical Organizational Culture: Refinement of a Scale. The Journal of applied behavioral science

Deloitte Report (2006). Deloitte global financial report. Retrieved from www.deloitte.com

Dhillon, Gurpreet., & Backhouse, James (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

Eloff, J. H., &Eloff, M. (2003). Information security management: a new paradigm. In Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology (pp. 130-136). South African Institute for Computer Scientists and Information Technologists.

Ethical Decision Making Framework Guide & Worksheets (2008) Toronto Central Community Care Access Centre Community Ethics Toolkit

Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security*, *13*(2), 113-170.

Ferrel, O.C., Fraedrich, J. & Ferrell, L. (2011). *Business Ethics. Ethical Decision making and Cases. Mason: South-Western Cengage Learning.*

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal*, *23*(4), 367-376.

Gonzalez, J. J., &Sawicka, A. (2002).A framework for human factors in information security.In *WSEAS International Conference on Information Security, Rio de Janeiro* (pp. 448-187).

He, Y., Johnson, C., Lu, Y., & Lin, Y. (2014). Improving the information security management: An industrial study in the privacy of electronic patient records. In *Computer-Based Medical Systems (CBMS), 2014 IEEE 27th International Symposium on* (pp. 525-526). IEEE.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003).An integrated system theory of information security management. Information Management & Computer Security, 11(5), 243-248.

Information Security Handbook. Retrieved from http://ishandbook.bsewall.com/

Islam, S., & Houmb, S. H. (2010, May). Integrating risk management activitiesinto requirements engineering. In *Research Challengesin Information Science (RCIS), 2010 Fourth International Conference on* (pp. 299-310). IEEE.

ISO, B. (2000). IEC 17799: 2000–BS 7799/1: 2000 BS ISO.

ISO/IEC 17799.(2000). p. viii

ISO/IEC 27001:2005. (2005). 'Information technology- security techniques- information security management systemsrequirements', Geneva: International Organization for Standardization.

Kaptein, M. (2008). Developing and testing a measure for the ethical culture of organizations: The corporate ethical virtues model. Journal of Organizational Behavior, 29(7), 923-947.

Karn G. Bulsuk (2009) Taking the First Step with the PDCA (Plan-Do-Check-Act) Cycle. Retrieved from http://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html (29 October 2014)

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. computers & security, 28(7), 509-520.

Kruger, H. Kearney, W. (2006). A prototype for assessing information security awareness. Science Direct.Vol.25, Issue 4, Pages 289-296

Kuzma, J., Paradise, J., Ramachandran, G., Kim, J., Kokotovich, A., & Wolf, S. M. (2008). An integrated approach to oversight assessment for emerging technologies. *Risk Analysis*, *28*(5), 1197-1220.

Loudon, K. C., & Loudon, J. P. (2002). Managing The Digital Firm.

Mason, R. O. (1986). Four ethical issues of the information age.Mis Quarterly, 5-12.

McConnell, L., &Wansley, M. (2011). Ethical Communication in the 21st Century.

Merkow, M. S., & Breithaupt, J. (2014). *Information security: Principles and practices*. Pearson Education.

Novelskaite, A., & Pucetaite, R. (2014). Validation Of Data Collection Instrument For Measurement Of Ethical Organizational Culture In Lithuanian Organizations. *Economics And Management*, *19*(3), 290-299.

Palm, E., & Hansson, S. O. (2006).The case for ethical technology assessment (eTA).*Technological forecasting and social change*, *73*(5), 543-558.

Peltier, T. R. (2005).Implementing an Information Security Awareness Program. Information Systems Security,14(2), 37-49.

Potter, C., & Beard, A. (2010). Information security breaches survey 2010.*Price Water House Coopers. Earl's Court, London*.

Quinn, M. J. (2014). *Ethics for the information age* (Vol. 4). Pearson.

Richardson, R. (2011). 2010/2011 CSI computer security crime security survey. Computer Security Institute.

Rungta, S., Raman, A., Kohlenberg, T., Li, H., Dave, M., &Kime, G. (2004). Bringing Security Proactively Into the Enterprise.Intel Technology Journal, 8(4).

Shinder, D. (2005). Ethical Issues for IT Security Professionals.*URL: www. windowsecurity. com/articles*.

Social scientific perspectives. Stanford: Stanford Business Books.

Suryawanshi, V., Mavkar, R., & Yadav, K. (2012). Ethical Implications to Hack & Issues in Information Security. *Advances in Computational Sciences & Technology, 5*(2).

Susanto12, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five.

Taherdoost, H., Sahibuddin, S., Namayandeh, M., &Jalaliyoon, N. (2013). Computer and Information Security Ethics--Models. In *Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on* (pp. 145-149). IEEE.

Tarimo, C. N. (2006). ICT security readiness checklist for developing countries: A social-technical approach.

Tarimo, C. N., Bakari, J. K., Yngström, L., & Kowalski, S. (2006). A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards a Culture of ICT Security-The Case of Tanzania. In *ISSA* (pp. 1-12).

Tiwary, D. K., & Pradesh, U. (2011). Security And Ethical Issues In It: An Organization's Perspective. *International Journal of Enterprise Computing and Business Systems, 1*, 10-20.

Treviño, L., & Weaver, G. (2003). Managing ethics in business organizations:

Tu, Z., & Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management: A Literature Review.

Van Kessel, P. (2011). Into the cloud, out of the fog: Ernst & Young's2011 Global Information Security Survey.

Vermeulen, C., & Von Solms, R. (2002).The information security management toolbox–taking the pain out of security management. Information Management & Computer Security, 10(3), 119-125.

Von Solms, B. (2001). Information security—a multidimensional discipline. Computers & Security, 20(6), 504-508.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Warren, E., Justice, C., & Supreme, U. (2005).Legal, Ethical, and Professional Issues in Information Security.

Werlinger, R., Hawkey, K., and Beznosov, K. (2009). An Integrated View of Human, Organizational, andTechnological Challenges of It Security Management.*Information Management & Computer Security*(17:1), pp 4-19.

Whitman, M., & Mattord, H. (2011). *Principles of information security*. Cengage Learning.

Whitman, M., & Mattord, H. (2013). *Management of information security*. Cengage Learning.

Woodhouse, S. (2007). Information security: end user behavior and corporate culture. In *Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on* (pp. 767-774). IEEE.

Wright, D. (2011). A framework for the ethical impact assessment of information technology.*Ethics and Information Technology*, *13*(3), 199-226.

Zaini, M. K., &Masrek, M. N. (2013).Conceptualizing the Relationships between Information Security Management Practices and Organizational Agility. In Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on (pp. 269-273). IEEE