A MODEL OF FACTORS INFLUENCING INFORMATION SECURITY CULTURE IN OIL AND GAS COMPANY

SURIANI BT MOHD

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

Advanced Informatics School
Universiti Teknologi Malaysia

JUNE 2017

“My dearest mum and dad, family, and friends”

This is for all of you

ACKNOWLEDGEMENT

Firstly, Gratitude and Thanks to the Almighty God, for his blessing. A world of thanks to my parents and family members that support me throughout my life and my studies. Deepest and sincere gratitude to my Supervisors Assoc. Prof. Dr.Nor Zairah Binti Ab.Rahim for her assistance and guidance throughout this research. Finally, thanks to all my course mate and friends for their support an encouragement

ABSTRACT

This research first identifies the factors that influence information security culture in private sector, specifically in one oil and gas company, followed by proposing a Factors Influence Information Security Culture Model. This research implemented quantitative methodology whereby an online questionnaire was distributed all employees in this company. All level respondent is included, from managerial level to non-executive staff. From the literature review it has been found that nine factors influence information security culture, however only five factors selected and tested in this research. Five factors are; top management support, security policy enforcement, security behaviour, security training and security awareness. These factors are tested on result of the survey of 70 respondents, five factors that influence information security culture is determined.

ABSTRAK

Kajian ini bermula dengan mengenal pasti faktor- faktor yang mempengaruhi budaya keselamatan maklumat di sektor swasta, secara spesifiknya di sebuah syarikat minyak dan gas, diikuti dengan cadangan Model Faktor-Faktor Yang Mempengaruhi Budaya Keselamatan Maklumat. Kajian ini melaksanakan kaedah kuantitatif dimana soalselidik diedarkan melalui atas talian kepada semua pekerja di syarikat ini. Semua peringkat responden termasuk, iaitu dari pihak pengurusan hinggalah kepada pekerja bukan eksekutif. Daripada rumusan penyelidik, didapati sembilan faktor yang mempengaruhi budaya keselamatan maklumat, namun hanya lima fakor sahaja yang dipilih dan dikaji dalam kajian ini. Lima faktor tersebut adalah sokongan pengurusan atasan, penguatkuasaan polisi keselamatan, kelakuan keselamatan, latihan keselamatan dan kesedaran keselamatan. Faktor-faktor ini dikaji keatas responden-responden di sebuah syarikat swasta iaitu daripada industri minyak dan gas untuk melihat adakah ia mempengaruhi budaya di syarikat tersebut.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREAVIATIONS

CIO	-Chief Information Officer
HIS	-Health Information System
ICSA	-Information Security Culture Assessment
IT	-Information Technology
ITDM	-Information Technology Decision Maker
ISC	-Information Security Culture
ISCF	-Information Security Culture framework
KM	-Knowledge Management
MyCERT	-Malaysia Computer Emergency Response Team
NIST	-National Institute of Standard and Technology
UAI	-Uncertainty Avoidance Index

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.0 Overview

Information is a very important asset for an organization. It is one of the caused or factor to the rise and fall of an organization. Therefore, the protection of the information and information asset from any forms of threats such as theft, breakage, leakage, unauthorized modification and disaster is crucial. The threat to the information and information asset security is not only caused by an external factor alone, on the other hand, the internal factors also influence and contribute to crime in the world of information technology or cyber. Hence the information security is very important to be cultivated and applied in an organization to make it a natural aspect of the daily activities of all employees or an individual in an organization. The culture will indirectly increase the knowledge of an individual's in regards to the cybercrime and the protection. Early prevention will avoid and close the opportunity of the crime from occurring which ultimately resulted in a loss to organizations and individuals.

1.1 Background of the problem

Modern organizations rely on information systems (IS) for their survival; this is because such systems often hold valuable organizational data resources (P. Ifinedo, 2012).Information system is much more than computer hardware; it is the entire set of software, hardware, data, people, procedures and networks necessary to use information as a resource in the organization.These are six critical components and each of the components has its own strengh and weaknesses.Often overlooked in computer security consideration,people have always been a threat to information security. People can be the weakest link in an organization's information security program. (Whitman and Mattord, 2005). It has been reported that one of the reasons why IS security incidents and abuses continue to plague organisations is that organisational employees are the weakest link in ensuring IS security; they constitute an insider threat to their organisations. (P. Ifinedo, 2014.)

According to the research of Italian psychologies only a quarter of corporate employees may be reputed as reliable, the same number of employees waits for a chance to disclosure information, and (50%) of employees will act depending on the situation. The Global State of Information Survey 2014 found out that the basic reasons of incidents in this filed are employees (31%) and former employees (27%). Financial losses due to the leakage of confidential information were 25 billion dollars in 2013, and this figures tend to grow. Confidential information theft leads to more significant effect. The best-known examples are the following: WikiLeaks published hundreds of thousands documents of participating the USA in war actions in Afghanistan, Iraq; the information containing PIN codes for 7 thousand Alfa-bank credit was stolen; E. Snowden revealed data of the US National Security Agency and so on. (Epifantsev, et al, 2016)

The public may imagine these cases to be the work of brilliant super-hackers coding through the night, the truth is more pedestrian: Each exploited human factors. The HBGary take down hinged on the victims' deplorable computer hygiene and the astonishing credulity of one executive, while WikiLeaks was the work of a disgruntled U.S. Army Private with an extraordinary degree of access. Even the largest and most sophisticated breach yet known the widespread penetration of U.S. and foreign agencies and defense contractors in a six-year effort believed to be backed by a foreign government reportedly relied heavily on social engineering and other human exploits. These cases offer vivid proof that corporations and governments today face great risk from members of their own organization. (Glassmeyer, 2011).

Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security. Without an adequate level of user cooperation and knowledge, many security techniques are liable to be misused or misinterpreted by users. This may result in even an adequate security measure becoming inadequate.(Niekerk and Solms, 2010).As stated by P.Ifinedo (2012), organizations often utilize a variety of tools and measures such as installing firewalls, updating anti-virus software, backing up their systems, maintaining and restricting access controls, using encryption keys, using surge protectors, and using comprehensive monitoring systems however, the aforementioned tools and measures offer a technological or technical solution to the problem, and are rarely sufficient in providing total protection of IS.

An organization's information security strategy should thus comprehensively address 'human factor' (Niekerk and Solms, 2010). One way of addressing the human aspect is to embed an information security culture where the interaction of employees with information assets contributes to the protection of these assets. Organization need to ensure that their employees are aware of information security and privacy policy requirements which encapsulate regulatory requirements. Employees needs to understand the risk to the information they process, implement the required control to protect it and take accountability for their action (Veigaa and Martin, 2015). Many recent studies have shown that the establishment of an information security culture in the organization is necessary for effective information security. Through the establishment of such a culture, the employees can become a security asset, instead of being a risk (Niekerk, and Solms, 2010). Culture, when it comes to security, includes the beliefs, values or behaviour with regard to security, or the behaviour in protecting the information assets of an organization. The behaviour of employees is influenced by their values and beliefs with regard to information security on the one hand and by the organization’s policies on the other hand. As such the behaviour of employees and the number of incidents that occur in the organization will portray the information security culture of the organization. (Shahibi, *et al.*2014). The study of information security culture and the factors influence the culture is therefore conducted in order to assist an organization to build the culture.

1.2 Statement of the Problem

Most of the organization today are fully dependent on information technology and system for their survival. Information system has become critical success factor to them. However, the increase of attacks and threats to information has made a protection to information and information asset as a great challenge. The rapid changes and progress in the information technology make it more difficult for the organization to maintain their protection towards the information and its critical asset. Base on the study conducted, it was found that the biggest threat to information confidentiality, availability and integrity are the organizational own employees. Along with technology and process, human is the biggest factor and weakness to information security. To overcome this issue, researcher, has suggested, the most effective way of organization to protect the information, information asset and ensure the compliance is for the executive management to promote security culture in the organization to be daily activities and a part of administration practice. This is due to human behaviour, lack of awareness, knowledge, belief and attention given to information security. To achieve this, it is necessary to integrate and adopt security into an organizational culture.

1.3 Research Questions

A study will be conducted to answer the main concern, question and to identify the Factors That Influence Information Security Culture in private sectors in Malaysia specifically in oil and gas company.

The main question for this studies are;

i) What are the factors that influence information security cultures in oil and gas company?
ii) How to design a conceptual model of factors influence Information security culture for this organization?
iii) How to evaluate the proposed model?

1.4 Research Objectives

The primary objective of this study is to identify factors that influence information security culture in private sectors in Malaysia specifically in oil and gas company, and below are additional objectives that will support the main purpose of this study.

i) To identify the factors that influence information security culture in in oil and gas company
ii) To identify a model for studies on factors influence information security culture
iii) To evaluate the proposed factors, influence information security model in this oil and gas company

1.5 Scope of the study

Target and scope of this study is one oil and gas company in Malaysia, focuses both on management and employees, because each responsible for the creation, dissemination and protection of the information and organization asset. The involvement of all level of employees contributed to the study as the employee are the primary creator and user of the information. Employees are from management level to non-executive level. Each of employee is assigned one computer for their works, hence the survey is distributed by online.

1.6 Significance of the Study

It is necessary to identify the factors influence information security culture because these factors contribute to form the culture in an organization. The factor that derived from this study can be compared to the existing factor in different area. The outcome of the study could be used to addressed and promote information security culture in the organization.

1.7 Summary

This chapter provide a brief discussion on the information security threat in an organization. It is concluded that human is a biggest threat, both internal and external of the organization. Based on studies, it is suggested that organization adopted security as part of its culture. For that reason, this studies is conducted to identify the factor that influence information security culture in an organization. The problem, objective and the significant of this studies has been presented in this chapter.

REFERENCES

A. B. Shahri, Z. Ismail, and N. Z. A. Rahim, *"Security culture and security awareness as the basic factors for security effectiveness in health information systems,*" J. Teknol. (Sciences Eng., vol. 64, no. 2, pp.7–12, 2013.

Akhyari Nasir, Ruzaini Abdullah Arshad, M. T. A. B. (2016). E*xploring Studies of Information Security Culture in Malaysia ICET 2016*. Exploring Studies of Culture in Malaysia, (August), 1–6.

AlHogail, A. (2015). *Design and validation of information security culture framework.* Computers in Human Behavior, 49(2015), 567–575.

Alhogail, A., & Mirza, A. (2014). A framework of information security culture change. Journal of Theoretical and Applied Information Technology, 64(2), 540–549.

Al-Mayahi, Alnatheer, Mohammed, Chan, Taizan,Nelson, Karen, (2012) Understanding And Measuring Information Security Culture

Al-Mayahi, I., & Mansoor, S. P. (2013). Information security culture assessment: Case study. In 2013 IEEE Third Int. Conference on Information Science and Technology (ICIST), 789–792. IEEE.

Alnatheer, Mohammed, Nelson, Karen (2009), Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context

Alnatheer, Mohammed, (2014) Conceptual Model to Understand Information Security Culture

B. N. Epifantsev, S. S. Zhumazhanova, and P. S. Lozhnikov, "*Insider threats to information security: Problem areas in neutralization,*" Int. Conf. Young Spec. Micro/Nanotechnologies Electron Devices, EDM, vol. 2016–August, pp. 133–136, 2016.

Control, D. (2013). Is Your Organization "Conversation Ready"? *2016 Data Security Incident Response Report*, 62–65.

Computer World 2016, Computer Security Summit 2016, Retrieved from http://www.computerworld.com.sg/microsites/cws/security-summit-2016-main/

Doug, Howard, Kevin Prince. (2011) Security 2020; Reduce Security Risk This Decade. Indianapolis. Wiley Publishing Inc.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers and Security*, *29*(2), 196–207.

Fourie, L. C. H. (2003). The management of information security--A South African case study. South African journal of business management, 34(2).

Ele, A., Veiga, D., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. Computer Law & Security Review, 31, 243–256.

E.Whitman,Michael & J.Mattord,Herbert (2005) Principle of Information Security. Boston. Massachusett.Thomson Course Technology

Eloff, J H PLim, Joo SChang, Shanton,Maynard, Sean.Ahmad, Atif (2009),Exploring the Relationship between Organizational Culture and Information Security Culture

Glassmeyer/McNamee Center for Digital Strategies (2011); Human Behavior and Security; Culture Human Behavior and Security Culture Managing Information Risk through a Better Understanding of Human Culture. Tuck School of Business at Dartmouth.

Hagen, J. M., Albrechsten, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Info Mngmt and Comp Security, 16(4), 377–397

IT Governance Institute; Information Security Governance; Guide for Board of Directors and Executive Management.2nd Ed. United Stated America.

IBM-Security. (2016). Reviewing a year of serious data breaches, major attacks and new vulnerabilities: Analysis of cyber-attack and incident data from IBM's worldwide security services operations. *IBM X-Force® Research 2016 Cyber Security Intelligence Index*, 1–19.

Kissel, R. (2013). Glossary of Key Information Security Terms Glossary of Key Information Security Terms. Nist, NISTIR 729(Revision 2).

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. Information Management & Computer Security, 14(1), 24-36.

Kuusisto, Tuija Ilvonen, Ilona.(2003) Information Security Culture in Small and Medium Size Enterprises

Lalitha Muniandy (2012). State of Cyber Security and the Factors Governing its Protection in Malaysia.International Journal of Applied Science and Technology. (Vol 2), 106-112

Laura Corriss, (2010) Information Security Governance: Integrating Security into the Organizational Culture. PP. 38–41.

Leedy,P.D (2001).Practical research: Planning and Design.7th Edition. Upper Saddle River, NJ, Prentice Hall

Martins, Ad'ele and Eloff, Jan (2002) Information Security Culture

Mark,Ciampa, (2010).Security Awareness: Applying practical security in your world. Boston; Course Technology.

Merete Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security, 16(4), 377-397.

Michael P.Gallagher, Albert N.Link,Brent R.Rowe. (2008), Cybersecurity, Cheltenham: Edward Elgar Publishing Limited.

Harris, M. A., & Reserved, A. R. (2010.). The Shaping of Managers Security Objectives Through Information Security Awareness Training.

MyCERT Incident Statistics 2015, Reported Incident based on General Incident Classification Statistics 2015, Retrieved from https://www.mycert.org.my/statistics/2015.php

M. S. Shahibi, R. M. R. S. K. W. Fakeh, and W. A. K. W.D. J. Ali, (2012) “Determining Factors Influencing Information Security Culture Among ICT Librarians,” vol. 37, no. 1.

N. H. Hassan and Z. Ismail, (2012) “A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment,” Procedia - Soc. Behav. Sci., vol. 65, no. ICIBSoS, pp. 1007–1012,

N. H. Hassan, Z. Ismail, and N. Maarop, (2014) “Understanding Relationship between Security Culture and Knowledge Management,” Knowledge

Management in Organizations Lecture Notes in Business Information Processing. pp. 397–402.

N. H. Hassan, Z. Ismail, and N. Maarop, (2013) “A conceptual model for knowledge sharing towards information security culture in healthcare organization,” 2013 Int. Conf. Res. Innov. Inf. Syst., vol. 2013, pp. 516–520.

Hassan, N. H., Ismail, Z., & Maarop, N. (2015). Information Security Culture: A Systematic Literature Revier. *Proceedings of the 5th International Conference on Computing and Informatics, ICOCI 2015*, (205), 456–463.

Ngo, L., Zhou, W., Chonka, A., & Singh, J. (2009). Assessing the level of I.T. security culture improvement: Results from three Australian SMEs. IECON Proceedings (Industrial Electronics Conference), 3189–3195.

P. Ifinedo, (2012) “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory”. Computers & Security, Vol 31, pp. 83–85.

P. Ifinedo, (2014) “Information & Management Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition,” Inf. Manag., vol. 51, no. 1, pp. 69–79.

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: Increased trust by an appropriate information security culture. *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA, 2003*–January, 405–409.

Abraham, S. (2013). Exploring the effectiveness of information security training and persuasive messages. *Dissertation Abstracts International Section A: Humanities and Social Sciences*.

Shahibi, M., Rashid, R., Wan Fakeh, S., Dollah, W., & Ali, J. (2012). Determining Factors Influencing Information Security Culture among Ict Librarians. Journal of Theoretical and Applied Information Technology, 37(1), 132–140.

Schmidt, Mark B; Johnston, Allen C; Arnett, Kirk P; Chen, Jim Q; Li, Suicheng. (2008) Journal of Global Information Management 16.2 .

Ramachandran, S. (2008). Information security cultures of four professions: A comparative study. In 41st Hawaii International Conference on System Sciences, 1–10. Sabbagh,

Robert, More. (2011). Cybercrime investigating high-technology computer crime. Oxford; Anderson Publishing.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. Computers and Security, 29(4), 476–486.

Veiga, A. Da, & Eloff, J. H. P. (2007). An Information security governance framework. Information Systems Management, 24(4), 361–372.

Verizon. (2017). 2017 Data Breach Investigations Report, 74. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Vroom, C, & Solms, R. Von. (2004). Towards information security behavioral compliance. Computers & Security, 2004(23), 191–198.,

Wash, R., & Rader, E. (2015). Too Much Knowledge? Security Beliefs and Protective Behaviors among United States Internet Users. Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 309–325.

Williams, P. A. H. (2009). Capturing Culture in Medical Information Security Research. Methodological Innovations Online, 4(3), 15–26.

Zakaria, Omar, (2007) Investigating information security culture challenges in a public-sector organization: a Malaysian case. Royal Holloway.