FACTORS INFLUENCING DATA LEAKAGE BEHAVIOR IN MALAYSIAN ARMED FORCES

MOHD NAZRUL BIN MAT ZOM

UNIVERSITI TEKNOLOGI MALAYSIA

FACTORS INFLUENCING DATA LEAKAGE BEHAVIOUR INMALAYSIAN ARMED FORCES

MOHD NAZRUL BIN MAT ZOM

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

Advanced Informatic School
UniversitiTeknologi Malaysia

June 2017

DEDICATION

Specially dedicated to my lovely family.
Thank you so much for all of your strong support, endless love, trust, constantencouragement, and prayers throughout my studies.

ACKNOWLEDGEMENT

Alhamdulillah,

I wish to express my sincere appreciation, thanks to my honorable and knowledgeable supervisor, EncikSaifulAdlibin Ismail and Dr. NurazeanbtMaaropfor theiroutstanding supervision and approach, support and sincere guidance by which it has been possible for me to complete this thesis.

My deepest gratitude also goes to my beloved wife and friends, thank you for the encouragement, support for being my inspiration, for your understanding and for your endless love.

ABSTRACT

Freedom of access in the variouschannel and media has raised the profound effect on confidential data dissemination and its security. The scarcity of security awareness particularly in Malaysian Armed Forces personnel practices in handling confidential data remain of utmost. This research aims to identify factors influencing data leakage attributes in Malaysian Armed Forces. This is executed by designing data leakage model and evaluating the proposed model. A quantitative research methodology is employed whereby, 187 questionnaires were distributed to personnel in the Malaysian Armed Forces from Officers and NCO's rank. 100% responses rate was recorded. SPSS version 22 is used for analysis. The results revealed significant with strong positive correlation between the identified attributes, namely computer usage behavior, security knowledge, security awareness and policy acceptance and understanding are influencing the received control data leakage.This research may assist the Malaysian Armed Forces in secured practices acquired in handling organisation's valuable assets which requires special guardianship on its perseverance.

ABSTRAK

Kebebasanaksesmenggunakanpelbagaimedia sibertelahmenyumbangkepadakesan yang mendalamterhadappenyebaranmaklumatberdarjahdanisukeselamatannya.Kekurangan kesedaranetikateknologiterutamanya di kalangananggotaAngkatanTentera Malaysia dalammengendalikanmaklumatberdarjahmenjadiperhatianutama.Kajianinibertujuanu ntukmengenalpasti factor-faktorpenyumbangkepadaketirisan data dikalangananggotaAngkatanTentera Malaysia dalampengendalianmaklumatberdarjah.Inidilaksanakandenganmerekabentukdanmeni lai model factor ketirisan data yang dicadangkan.Kaedahpenyelidikankuantitatifdijalankan di mana 187 soalselidiktelahdiedarkankepadaanggota di dalamAngkatanTentera Malaysia berpangkatPegawaidan LLP. 100% kadarmaklumbalasdirekodkan. SPSS versi22digunakanuntukanalisis.Hasilkajianmenunjukkansignifikandengankorelasipos itifkukuhantaraciri-cirifaktorkesedarankeselamatan data di kalanganpekerja, kelakuanpenggunasemasamenggunakanperalatankomputer, pengetahuankeselamatan data danpenguatkuasaanpolisi di dalamorganisasi.KajianinidapatmembantuAngkatanTenteradalamamalanterbaikdala mmemastikankelangsungandalammengendalikanasetorganisasi yang bernilai yang memerlukanpenjagaanrapi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AFGI	-	Armed Forces General Instruction
CO	-	Commanding Officer
DISD	-	Defence Intelligence Staff Division
IV	-	Independent Variable
DV	-	Dependent Variable
MAF	-	Malaysian Armed Forces
NCO	-	Non Commission Officers
PICOC	-	Population, Intervention, Comparison, Outcomes and Context
SLR	-	Systematic Literature Review
MAMPU	-	National Security Council
FTP	-	File Transfer Protocol
ICT	-	Information And Communications Technology
HEI	-	Higher Education Instituition
IPVPN	-	Internet Protocol Virtual Private
DEMS	-	Defence Electronic Messaging System
C2	-	Command and Control
SETA	-	Security Education Training and Awareness

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Every industry sector including private and government around the world has faced the same problem which is confidential data leak, stolen and lost to the unknown parties. The result is cost of much money because of direct or indirect losses and also brings bad reputations and brands. (Young, 2010).Information security plays an important role in ensuring that all information is protected. Safety information is also referred as computer security is defined as protection granted to automated information systems to achieve the objective to maintain the confidentiality, integrity and availability resource information systems (Zafar, 2013). In other definitions, synonyms data leaks with a leak of information from the illegal transmission of information within an organization for destinations outside or receiver. Unauthorized transmission does not automatically mean an accidental or malicious (Institute, 2007).

Types of incidents have occurred which is sale of customer account personal detail to beneficial parties and the loss other media such as laptops, USB sticks, backup tapes and mobile devices. The majority of the incidents are caused by internal users and trusted third parties and most of them are unintentional (Young, 2010). Likewise, government business demands to embrace new technologies such as social media and mobile devices have made it impossible for most organizations to simply build and rely on a strong perimeter for adequate protection(Young, 2010).

The military information system is no exception. Military information is a

type of information use as medium to do daily routine works such as electronic document, instruction and command. Specifically if it is correlated with sovereignty of the country, tactics or strategy is compromised, the result will be connected to national security (Jung Ho Eom, 2012).

1.2 Background of the Problem

Data losses has caused adverse effects to the organization in terms of putting the organization's network and malware risk system, which led to legal action that has the potential for copyright, loss of production and will affect the organization's brands and sales front (Colwill 2010; Gudaitis, 2010; Young, 2010).

More recently, data losses by cyber criminals not focus to steal confidential information, but use them for botnet command and control (Everett, 2010; Smith & Koppel, 2009; Westervelt, 2009). Worsen that, Facebook profile is currently available for download through the website, sharing disclosing information more than 170 million users worldwide (Paul, 2010).

Moreover, cyber criminals today are more interested in collecting information, the organization, from the famous to take down the network (McAfee, 2010). They were certain sponsored parties that perform highly skill attack to steal valuable datain the organizations use their employee as target. They use the data available in public domain, particularly online social media account to get much information about important person before launching spear phishing techniques and social engineering to get the partial information to access important data (Smith & Koppel, 2009; Sophos, 2010; Symantec, 2015).

Thus, small or large organizations, government agencies or private companies, need to pay close attention to medium of data being loss among their employees. They cannot rely solely on technical controls to combat this problem because it involves human that need to be covered by policy and procedures.

In Malaysia, a study from the National Security Council (MAMPU) and the MAMPU concerning electronic data leakage in the government sector for the year 2012 found that almost 50% of the source of leakage is of email (MAMPU, 2013).

Most government departments in putting into their information security policies on the importance of data leakage, but some of them do not implement the solution. The problem is that most users do not realize the impact of the leak. It has been proven by a study conducted by the National Security Council and the MAMPU concerning electronic data leakage in the government sector (MAMPU, 2013). Table 1.1 shows the statistics of electronic data leakage in the government sector for the year 2012.

Table 1.1: Statistics of Electronic Information Leaks in the Government Sector in 2012 (MAMPU, 2013)

Medium / Source	**(%)**
E-mail	50
Laptop Computer	48
Internet	46
USB media	43
Remote Access by Service Provider	42
Smart Phone	41
Desktop Computer	40
External Storage Media	39

Source :MAMPU, 2013

The most significant result of the leakage of data, including substantial financial impact due to loss of intellectual property, other than that, information leaks can also cause financial losses, damage to the reputation of the government, remained negative publicity and loss of or damage to sensitive information and damage to the reputation of the government through information disclosure Sensitive to the public or unauthorized recipients (Technology, 2009). It is important

to realize that technology is only as effective as the people and the process behind it. Human error, ignorance, omission, or failures to comply with the policies that are available are most of the time the cause of data breaches and information leaks (Marko and Martijn, 2012).

The incident occurred will damage the shield of confidentiality, integrity and availability of the organization. Usually it is caused by human error and technology. Employees are the key factors that can cause great harm to the confidentiality, integrity, or availability of information through intentional activities. Thus, the behavior of the human factor should be changed to ensure standard practices carried out in handling information assets. The level of awareness among workers should be strengthened within the organization.

From the Malaysian Armed Forces (MAF) views, it has been incident triggered to the development of ethics and policies in handling confidential information. Armed Forces General Instruction's (2013) (AFGI) (Secretariat, A., 2013)stated that information contamination include the activity which is intentionally or unintentionally that encourage to the military information leakage, open criticize or give opinion or overview on military and government basis, sensitive sentiment that can occur individual hatred on military and government policy and things can jeopardized our own country sovereignty and safety.

(Secretariat, A., 2013)also stated a few method and action that will be classified as information contamination:

i. Uploading, view, update or transmitted any form of classified or degree document.

ii. Downloading any form of application and any document from unknown sources and did not know about their security clearance.

iii. Discussing and take part into the forum that can lead to compromise national security and harmony.

iv. Instigate or offer to any form of provocation.

v. Use public email for official use.

vi. Using public web hosting to host official company website.

vii. To allow third party do the ICT audit, penetration testing and have access to company internal system without BSPP permission.

viii. Provided Wi-Fi Access Point in the building, premises, and between MAF compartments without BSPP permission.

ix. Use official and unknown free Wi-Fi to conduct with security classification document.

x. Store any official and work related in personal computer.

xi. Reconnect intranet connection to public internet connection without administrator or BSPP permission.

Seen from the exposure threats of unauthorized access such as hacking, fraud, counterfeiting, interception, data disclosure, and malicious code (Cobb and Lee, 2014) along with Electromagnetic Pulse, Ionizing Radiation, Electromagnetic Compatibility and Radio Frequency Interference, threats are all vulnerable to the information technology systems (Hoad and Jones, 2004) which is capable in affecting data confidentiality, integrity and availability. The existence of new methods intrusion into a formidable ICT network has forced all levels of MAF personnel to inculcate ICT security culture in handling the confidential information.

1.3 Problem Statement

Military information is one of the important data/information in MAF. The usage of the device and technology has uncontrollable, insiders and external threat, among staffs and this situation created a challenge to MAF to contain and secure the confidential data. It is very important that data leakage factors needs to be properly

addressed in order to minimize the leakage. This can help MAF Higher Authority in effective use of the strategy and its control on leakage. The main issue is to propose an evaluated model for the data leakage in MAF to address components and security issues with regards to data leakage.

Through preliminary interviews, it can be concluded that the MAF struggle and tried harder to achieve and maintain confidential information superiority due to the technology development. This may be difficult to achieve because some of the personnelnot proper handling the data by not obey the policies and taking serious compliances in its preservation. Personnel mishandling confidential information/military information is the largest contributor to the data leakage to the third parties instead of the effort in prohibiting the threats, exploitation and the outsider intervention, (Secretariat, A., 2013).

1.4 Research Questions

There are several research questions that had been identified in order to develop research objectives. To sum up, the study is to explore some answers to the following questions:

i. What are the data leakagesfactors among personnel of the MAF?

ii. How to develop conceptualdata leakage model for the MAF?

iii. How to evaluate the proposed conceptual data leakage model in MAF?

1.5 Research Objectives

Upon completion of this study, there are three objectives that need to be achieved. They are as:

i. To identify the factors of data leakageamong personnel of the MAF.

ii. To develop a conceptual data leakage modelfor MAF.

iii. To evaluate the conceptual data leakage model for MAF.

1.6 Research Aim

The aim of this research is to identify the data leakage component in organization, to design and evaluate the data leakage conceptual model for the Armed Forces. The tested model serves to assist the MAF's superior in identifying the baseline required for each MAF personnel in practicing the most secured way in handling a data from being leaked along with factors of data leakage attributes found in this research.

1.7 Research Scope

Scope of research sets the boundaries of the study. The following outlines the limitations:

i. Unit of analysis are MAF Personnel at MAF Headquarters taking into consideration that handling confidential and sensitive data.

ii. Data collection is by quantitative method, using self-administered questionnaire.

iii. Data analysis using SPSS Version 22.

1.8 Significance of the Research

This section discusses the significance of the study from the methodological, theoretical and practical viewpoints.

1.8.1 Methodological Contribution

As there is a lack of study using quantitative analysis on data loss in military environment, therefore this research attempts to provide more information on factors influencing data leakage in MAF organisation. The survey focuses on MAF Personnel at MAF HQ.

1.8.2 Theoretical Contribution

Several models gathered from the theoretical academic standpoint were referred which are among them are the model of antecedent and outcome of Model for Factor Influencing Information Security Factor introduced by Hassan & Ismail. (2012), the model Of Managerial Effectiveness in Information Security introduced by Knapp (2005), Framework for controlling insider threats to information security introduced by Yayla (2011). The model is then consecutively being compared and the relationship is mapped along with attributes found on the Systematic Literature Review (SLR). These steps are achieved by the availabilities of the model presented by previous researches towards the potential identification of the deliverable. Therefore, these model are integrated and tested in a military environment.

1.8.3 Practical Contribution

This research will be served as a direction to the managerial perspective of the Armed Forces organisation in viewing the attributes of data leakage behaviour in MAF. With the to-be distributed Armed Forces Security Instruction, the outcome of this research will comprise of the attributes among the selected population that can be further measured to others military organisation in a wider scope. It will help the policy maker to make strategic assumptions towards the refinement of the MAF personnel in handling the confidential data which are known to be sensitive information from the derived model.

It is furthermore equipped an insight that enables the management to strategically formulate the policies creation, personnel privileges management, planning for better training and awareness program checklist and personnel employment screening including personnel background checks towards instilling a strong security culture in the MAF environment. The contribution would instantaneously impress the strategic managerial to respond with the practical implementation of the betterment of the whereabouts, footing, and setting of the organization.

1.9 Organization of the Thesis

This report consists of five chapters and the entire chapters are organized according to the flow of the works involved. Chapter one outlines the overview section, and then it continues with the problem background of this research followed by problem statements, research questions, aim, objective, scope and significance of the study.

Chapter two reviews the literature review related to the study area, which is a data leakagemodel in MAF that relate to each topic. It discussed the previous researcher work in component and its problem, and then the proposed data leakage behavior model for MAF.

Chapter three explains method used in the study and operational framework. This chapter describes in details all processes involved in the study on form of work flow.

Chapter four discusses the findings and analysis that from questionnaires to evaluate the proposed model.

Lastly, chapter five conclude overall of the project. Research achievement, challenge and constraint while carrying out the research and future recommendation of the study will be discuss. A summary of the research project will be concluded in this chapter.

REFERENCES

Ajzen, I. (1991). *The Theory of Planned Behaviour.OrganisationalBehaviour and HumanDecision Process*, 50(2), 179- 211.

Alexa.(2011). Global top sites. From http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

BBC. (2010). Israeli military 'unfriends' soldier after Facebook leak from http://news.bbc.co.uk/2/hi/middle_east/8549099.stm

Bulgurcu, B., Cavusoglu, H., &Benbasat, I. (2010). Information Security Policy Compliance: *An Empirical Study of Rationality-based Beliefs and Information Security Awareness*. MIS Quarterly, 34(3), 523-548.

Chang, S. H., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems.

Colwill, C. (2010). *Human factors in information security: The insider threat - Who can you trust these days?* Information Security Technical Report, in press.

Comerford, J. D. (2006). Competent computing: A lawyer's ethical duty to safeguard the confidentiality and integrity of client information stored on computers and computer networks. The Georgetown Journal of Legal Ethics

Dhamija, R., Tygar, J., & Hearst, M. (2006). Why phishing works. Proceedings of the SIGCHI conference on Human Factors in Computing Systems.

Dhillon, G., &Torkzadeh, G. (2006).Valuefocused assessment of information system security in organizations. Information Systems Journal

Everett, C. (2010). *Social media: opportunity or risk?* Computer Fraud & Security, 8-10.

Gudaitis, T. (2010).*The Impact of Social Media on Corporate Security: What Every Company Needs to Know*. Cyveillance, Inc.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems

Institute, S. (2007). *Data Leakage - Threats and Mitigation*.SANS Institute.

Knapp, K. N., Morris Jr., R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers & Security.

Lean-ping, O., &Chien-fatt, C. (2014).*Information Security Awareness : An Application of Psychological Factors – A Study in Malaysia*, (Ccit).

McAfee. (2010). Protecting Your Critical Assets: Lessons Learned from "Operation Aurora": McAfee, Inc.

Moen, V., Klingsheim, A. N., Simonsen, K. F., & Hole, K. J. (2007).Vulnerabilities in egovernments.International Journal of Electronic Security and Digital Forensics.

Nor, F. M. F. (2014).*Factors Influencing Implementation Of Information Leakage Prevention For Government Sector*. Thesis Master of Science, UniversitiTeknologi Malaysia.

Paul, I. (2010). The Facebook data torrent debacle: Q&A. PCWorld.

Smith, A. M., &Toppel, N. Y. (2009*). Case study: Using security awareness to combat the advanced persistent threat*. Paper presented at the 13th Colloquium for Information Systems Security Education (CISSE), University of Alaska, Fairbanks, Seattle.

Solomon, M. G., & Chapple, M. (2005). Information Security Illuminated (Jones and Barlett Illuminated). Sudbury, MA: Jones and Bartlett Publishers, Inc

Sophos. (2010). Security Threat Report: 2010. Boston, Massachusetts: Sophos Group.

Straub, D. (1990). *Effective IS Security*. Information Systems Research, 1(3), 255-276.

Symantec. (2010). Symantec Global Internet Security Threat Report: Trends for 2009. California, U.S.: Symantec Corporation.

Theoharidou, M., Kokolakis, S., Karyda, M., &Kiountouzis, E. (2005). *The insider threat to information systems and the effectiveness of ISO17799*. Computers & Society 24, 472-484.

Titus. (2008). Best Practices for a Successful DLP Deployment.

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

Westervelt, R. (2009). *Botnet masters turn to Google, social networks to avoid detection*.http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1373974,00.html

Wilson, J. (2009). *Social networking: the business case*. Engineering & Technology (4)10 54-56.

Workman, M., &Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology*, 58(2), 212-222.

Yayla, A. A. (2011). Controlling Insider Threats With Information Security Policies.

Young, K. (2010). *Policies and procedures to manage employee Internet abuse*. Computers in Human Behaviour, 26, 1467-1471.

Zafar, H. (2013). *Human resource information systems: Information security concerns for organizations*. Human Resource Management Review, 23(1), 105– 113.

Zakaria, N. H., &Katuk, N. (2013).*Towards designing effective security messages: Persuasive password guidelines*. 2013 International Conference on Research and Innovation in Information Systems (ICRIIS), 2013, 129–134.