THE AWARENESS OF SECURITY BREACH AMONG USER IT IN KPTMBP

INTAN SAFINA BINTI OTHMAN

MASTER OF COMPUTER SCIENCE
(INTERNETWORKING TECHNOLOGY)

2016

Faculty of Information and Communication Technology

THE AWARENSS OF INFORMATION SECURITY BREACH AMONG USER IT IN KPTMBP

Intan Safina Binti Othman

Master of Computer Science (Internetworking Technology)

2016

THE AWARENESS OF INFORMATION SECURITY BREACH AMONG USER IT IN KPTMBP

INTAN SAFINA BINTI OTHMAN

A project submitted
in fulfillment of the requirements for the degree of Master of Computer Science
(Internetworking Technology)

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2016

DECLARATION

I declare that this thesis entitled "The Awareness of Information Security Breach among User IT in KPTMBP" is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ……..

Name : ……..

Date : ……..……

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in term of scope and quality for the award of Master of Computer Science in Internetworking Technology.

Signature	:	……..
Supervisor Name	:	……..
Date	:	……..……

ABSTRACT

Recently, network security has become a major concern in cyber world. Thus, the need in cyber security is higher in order to make our data safety and privacy. The usages of internet are widely used in internet banking, online shopping, data storage, global positioning system, media and many other social applications. Security became a critical aspect in an overall information security area. Human error becomes a vulnerable to security breaches if a user did not practice safety behavior. Therefore, this study was conducted to investigate the unsatisfactory factors towards individual, organization and information security awareness towards security breach among user in Kolej Poly-Tech MARA Batu Pahat (KPTM). By observing the literature review and related research, this study proposed a research model of the awareness of security breach relying on the individual, organization and information security awareness. In conjunction with proposed model, this study addresses 2 hypothesis which are; H_1- there is no relationship between independence variables and dependence variable; H_2- there is a relationship between independence variables and dependence variable. The descriptive research has been used to investigate awareness of information security that focus on human error, policy and procedure and information security awareness in education and experience by distributing the questionnaires. The respondents of this study involve 155 of user in KPTM that used techniques of snowballs to gather the data. This study might help IT Officer in Batu Pahat or others branches in KPTM to monitor the awareness level of users towards information security, thus can design an information security awareness programs like campaign, seminar and case study. Meanwhile, KPTM Batu Pahat also can design a more robust system policy and procedure that would ensure the systems with a condition of confidentiality, integrity and availability of the system. For future work, this study can be implement in different private and public colleagues and universities mainly at west region to cover a large population of sampling.

ABSTRAK

Umumnya, keperluan dalam keselamatan data telah menjadi fokus yang utama dalam rangkaian teknologi maklumat. Oleh itu, keperluan dalam menjaga keselamatan data dalam dunia teknologi maklumat amat diperlukan bagi menjadikan keselamatan data lebih effisen dan privasi. Internet telah digunakan secara meluas dalam perbankan internet, membeli-belah dalam talian, penyimpanan data jarak jauh, sistem kedudukan global, dan aplikasi sosial yang lain. Faktor utama yang menyumbang kepada pelanggaran keselamatan data adalah disebabkan tahap kesedaran yang rendah dalam individu, organisasi dan persekitaran. Oleh itu, kajian ini dijalankan untuk mengkaji faktor-faktor yang menjadi penyebab kepada pelanggaran keselamatan data di Kolej Poly-Tech MARA Batu Pahat (KPTM) sejajar dengan objektif utama yang telah digariskan iaitu mengkaji faktor-faktor yang menyumbang kepada pelanggaran data dengan memberi fokus kepada faktor individu, organisasi dan kesedaran keselamatan data dengan membangunkan satu model baru berdasarkan hasil kajian. Pembangunan model kesedaran keselamatan data berdasarkan 2 hipotesis utaman iaitu; H_1 – tiada hubungan di antara pemboleh ubah peramal dengan moderator; H_2- ada hubungan di antar pemboleh ubah peramal dan moderator. Hasil penilaian telah diperolehi dengan mejalankan kajian literatur dan kajian yang berkaitan dengan keselamatan data dengan mencadangkan satu model kajian yang akan mengukur tahap kesedaran pada individu, organisasi dan kesedaran keselamatan data terhadap keselamatan data di KPTM Batu Pahat. Kajian deskriptif pada soal selidik telah digunakan untuk mengkaji kesedaran keselamatan data dengan memberi penekanan terhadap keselamatan maklumat mengenai kesilapan manusia, polisi dan prosedur dan kesedaran pelanggaran data di KPTM Batu Pahat. Responden kajian ini melibatkan 155 daripada pengguna di KPTM yang menggunakan teknik bola salji untuk mengumpul data. Oleh itu, diharap hasil kajian ini dapat menyumbang kepada pegawai teknologi maklumat di KPTM Batu Pahat atau cawangan lain dalam menilai tahap kesedaran pengguna terhadap keselamatan data dengan membangunkan program kesedaran keselamatan data terhadap pengguna di KPTM. Selain itu, aspek aspek kerahsiaan; integriti dan kesediaan sesuatu sistem harus ada dalam membangunkan polisi dan prosedur. Dapatan daripada kajian, boleh di gunakan di universiti tempatan atau swasta fokus pada universiti atau kolej yang berada di sebelah selatan Malaysia untuk mendapatkan populasi yang lebih besar.

ACKNOWLEDGEMENTS

Bismilahirahmanirahim..

First and foremost, my appreciations thank to Allah Almighty, who made me capable to complete this project throughout those difficult years.

I would like to thanks to my project supervisor Assoc. Prof. Dr. Abdul Samad Shibghatullah for valuable guidance, constant support and outstanding supervision. I really appreciate and thank to him for suggestions and advice to provide a broad idea on this project. It is understood that without the advice and admonitions, my work will not be completed.

Special thanks to the lecturers of Faculty Information and Communication Technology (FTMK) and Centre for Graduate Studies (CGS) of Universiti Teknikal Malaysia Melaka (UTeM) for their assistance during this project.

I would also like to thank my fellow friends who had given encouragement and support to me. Finally, I would like to convey thanks to my beloved husband, parents and siblings who have supported me in the process of completing this project.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

p

LIST OF ABBREVIATIONS

IT	-	Information Technology
KPTM	-	Kolej Poly-Tech MARA Batu Pahat
1MDB	-	1 Malaysian Development Berhad
DOS	-	Denial of Services
DDOS	-	Distributed Denial of Services
IP	-	Internet Protocol
IP SeC	-	Internet Protocol Security
KAB	-	Knowledge and Behavior
TAM	-	Technology Acceptance Model
TPB	-	Theory of Planned Behavior
TRA	-	Theory of Reasoned Action
PBC	-	Perceived Behavior Control
DTPB	-	Decomposed Theory of Planned Behavior
HAIS-Q	-	Human Aspects of Information Security Questions

CHAPTER 1

INTRODUCTION

1.0 Background of the Study

The phrase of 'New Tools, Old Crime' is refer to the crime that occurs in cyberspace by using networking devices tools (Mohamed, 2013). Nowadays, the usage of internet are widely used. The technology shift make many companies appear to produces a variable types of devices like computer, mobile device, smart phones, tablets, iPad, and others mobile device that can be connected to the internet at any time and places. Internet give a lot of advantages to a user like access to the social media, chatting, purchase online product, online banking, watching video, sent email and many more. Although it solve many issues regarding the technology but it also create another problem if the user not have any knowledge towards information security (Tayouri, 2015).

This study is focusing on the awareness of security breach among user IT in Kolej Poly-Tech MARA Batu Pahat (KPTM BP). The most error done by user are; sharing password, open unknown email, leaving unattended workstation, updating status on media social and etc. Their actions towards information security vulnerable hacker's or attackers to penetrate into user's system. Once the attacker hijacking the system, data confidentiality, availability and privacy cannot be defend (Veiga and Martins, 2015). Moreover, if the organizational did not take major action aiming on information security, the organizational have to face the consequences like organizational asset loss.

Thus, the need on defense mechanism on information security must be tighten to prevent organizational assets loss. Organizational must enhance employee knowledge, adequate and understanding on information security and its challenge (Zainol et al., 2012).

1.1 Research Background

With the growth of internet, people around the world have use the internet as a medium to communicate, businesses, learning, online banking, cloud data storage, access to government website, applying work and etc. Hence, the defense mechanism toward security system must be tighten to ensure our communication system reach the standards and policies by Malaysian Communication and Multimedia Commission (SKMM). Phishing, DOS attack, eavesdropping, data modification, IP Spoofing, Man- in-the-middle attack, modification of data and phishing are an examples of security attack. The organization should take action to defense the system from attackers' activities. The activities contributes to security breach like unattended record files, carelessness, spamming, unstrengthen password and many more. They not only seek for the information but also have full access in our system once they penetrate into our environment (Zhiwei and Zhongyuan, 2012).

Employees are the major contributors in information security breach. Occasionally, their actions may deliberately effect on an organizational structure. An example of user misconduct are; employee carelessness, policies and procedure are not obligated, improper data storing, training are not conducted by an authorized personnel and many more. Nevertheless, employees itself might tend to employ information assets due it personal reasons like illegal access towards data confidentiality, fraud of data, malicious software, misuse and etc. (Zainol et al., 2012).

Human errors are the factors that produce threats in our information system. Internal threat is a person who have a motive to destructive the company because of dissatisfied like denied promotion or informed of employment termination organization and. Database breaches, fraud, theft, or blackmail are an example of internal threats. The power of an insiders attackers can disgruntled the company because they have an access to the company. For an example, an employee stealing company information and sell it to other companies (Montesdioca and Maçada, 2015). According to Xerox study, it has showed 51 percent of data duplication in company printer.

While, the external threats is a system expert that derived from an outside of organization. The modus operandi of the threats is to penetrate into the system by find the weakness of the system through the insiders' people. The most error contribute to the external threats is human carelessness like leave the equipment unattended, spamming spoofing, alteration of data and so on. The mistake made by human also possess the attacker to slip into the network. Once the attacker enter into system, they can do anything they want like view your information, blackmailing, sabotage and worst come to worst they can have full access on your system and can destroy information needed (Vladlena et al., 2015).

Moreover, the survey will be conducted to measure the relationship between independent variables and dependent variables that contribute to an awareness of information security breach. Before the analysis conducted, the factors that contribute to human error must be discover.

1.2 Problem Statement

In 2015, the growth of number on Malaysian cyber-crime has reach 10,636 cases comparable to last year data has stated 9,986 cases reported by Communication and Multimedia Deputy Minister, Dato' Jailani Bin Johari. On 26th January 2015, Malaysian Airline Website has been compromised through it Domain Name System reported by Star Online. On 15th December 2015, Internet security breach was detected on 1MDB. In 2011, KPTM web site has been hacked by the perpetrator.

According to (Parsons et al., 2014), human error can be recognized into seven focus areas which are information handling, password management, mobile computing, internet use, social networking use, incident reporting and email use. Interview with IT executive of KPTM Batu Pahat indicate that human error are commonly responsible for information security breach and this supported by (Parsons et al., 2014) and (Ahmed et al., 2012). Therefore, the development of the questionnaire based on the behavior, knowledge and attitude that associates with human error in computer usage or application. As a user of Internet, they must be knowledgeable and aware any kind of activities involved when deal with the internet. A user must bear in mind everything will became clear crystal to an attacker when we use the internet (Ifinedo, 2014). Thus, without awareness in cyber security user will give space to any kind of attacker to penetrate into our system without our knowing.

DOS, DDOS, MAN-IN-THE-MIDDLE-ATTACK, packet sniffing, virus, malware, network reconnaissance, phishing, scamming and many more are an example of network attacks. These attack will give various impact to our system. Once they penetrate to our system, they can read all the information in our system with or without destructing our system (Infrastructure and Group, 2002). Therefore, staffs, and students fail to identify factors that contribute to the human error among user IT in KPTM BP.

To address the research objective, the development of this study based on the research questions below:

i. What are the factors that contribute to the human error in security breach?
ii. Does policy and procedure contribute to the security breach?
iii. Does information security awareness affect the security breach?
iv. What are the reliability and consistency of the questionnaire?
v. Does independent variable and dependent variable correlate with each other?
vi. Does independent variable and dependent variable show a relationship toward security breach?

1.3 Research Objectives

The project objective aimed as follows:

i. To investigate the factors that contribute to human error among user IT in KPTM Batu Pahat.
ii. To design and develop a questionnaire that cover about security breach.
iii. To examine the relationship between independent variables and dependent variables that contributes to an awareness of security breach in KPTM Batu Pahat.

1.4 Research Methodology

A descriptive research study have been conducted to investigate the awareness level towards security breaches focusing on knowledge on policies and procedure; technology and system adaptation from Neil J. Salkind by using a questionnaire. Questionnaire is a tool that will be used to capture rich, detailed information that contribute to human behavior and knowledge towards policy and procedure in security breach among user IT in KPTM BP. By using descriptive quantitative research design the detailed information can be gather to design or adopt an exploratory approach regarding network security issues. To construct a questionnaire hybrid method will be used. The selected population of this study are categorized into education sector mainly have a knowledge in information technology focusing in KPTM BP. This study sample 30% of KPTM BP user mainly students and staffs that contributes to 330 respondents come from different background.

1.5 Expected Outcome

The expected outcome from this study might help IT officer in KPTM BP to focus on monitoring user behaviors and strengthen the policy and procedure thus design a more robust system that would ensure and enhance system with confidentiality, integrity and availability of information security. Besides that, the result from this study also can be used as a guideline for others branches of KPTM thus, will improve the design system; empowering; and monitoring control are improved.

1.6 Conclusion

This chapter has provided to presents the background of the project that describes a network security technology, the awareness of security breaches focusing on human error among user IT in KPTM BP. The description of problem statement and issue involve in security breaches causes by human error has been clearly identified and method to solve this problem also been discuss. The objective of this project clearly describe how to tackle this problem. Meanwhile, significance of this study also describe the benefit and purpose to students, staffs and IT Officers and others branch of KPTM. The expected outcome of this project clearly describe the importance of awareness of security breaches causes to human behavior can be gain by other investigator in the field of network security.

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

Computer Science fields can be categorized into several sections which are Computer Programming, Artificial Intelligent, Network, System, and Graphic. In spite of that, this study was focusing on Computer Network fields where it can be categorizes into Network Programming, Neural Network and Network Security. The domain of Computer Network Security are divided into web security, network security and system security. In this study, we are focus on Network Security, where in this domain it divided into subsection which are computer attack and its' defends methods. End-system was the vulnerable to an attacker and easily to exploit remotely (Chasaki and Wolf, 2012). Therefore, our focus on this study specialized on end-system attack rather than control plane attack and data plane attack. By referring the Cisco, Network Security can be refer as any activities used to protect your network in term of usability, reliability, integrity and safety of your data and network. The following Figure 2.1 and Figure 2.2 shows K-Chart diagram for our domain of study.

According to Cisco, threat nowadays, can be spread through the internet. Thus, the need to strengthen our network became a highly prioritized. To protect our network from any attacker or threats, software updates is needed. The defense method that we use to overcome the threats by using antivirus and anti-spyware programed, implement Firewall, Intrusion Prevention System and Virtual Private Network (tunneling protocol).

There are different types of threat that exist in our cyber world which are viruses, worms and Trojan horses, spyware and adware, zero-day attacks (zero-hour attack), hacker attacks, Denial of service attacks, data interception and theft and identity theft (Antunes and Vieira, 2012).

This study was conducted to investigate the factors that affect security breach focusing in human error. Observation on literatures survey have been conducted to identify the independent variable that donates to security breaches. The literature survey focus on work related to the awareness of information security mainly on human error aspect. Seven areas of human errors can be divided into information handling, password management, mobile computing, internet use, social networking use, incident reporting and email use adaptation from (Parsons et al., 2014) and (Pattinson et al., 1999).

The factors of information security awareness are discovered by observation on literature survey and an interview conducted with IT Officer. Secondly, the questionnaire will be develop according to independent variable and dependent variable. Then, the relationship between independent variables and dependent variable will be analyze by deploy Cronbach's alpha coefficient and correlation values, which has to exceed 0.7 for each major factors. This alpha value (0.7) indicated the strong positive multiple regression between dependent variable and independent variable.