FACTORS INFLUENCING EMPLOYEE BEHAVIOUR TOWARDS INFORMATION SYSTEM SECURITY (ISS) IN THE ORGANIZATIONS

NUR SHARLIN ARINA BINTI MD SUFFIAN

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FACTORS INFLUENCING EMPLOYEE BEHAVIOUR TOWARDS INFORMATION SYSTEM SECURITY (ISS) IN THE ORGANIZATIONS

NUR SHARLIN ARINA BINTI MD SUFFIAN

A report submitted

In fulfilment of the requirements-for the degree of

Bachelor of Technology Management (Innovation)

Faculty of Technology Management and Technopreneurship

Universiti Teknikal Malaysia Melaka

JUNE 2019

SUPERVISOR DECLARATION

" We hereby acknowledge that we had read this project paper and in our opinion, this work sufficient in terms of scope and quality for the award of Bachelor Technology Management (Innovation) with Honour"

Signature : …….

Supervisor's Name : Dr Nusaibah Binti Mansor

Date : …….

Signature : …..……....

Panel's Name : Dr Siti Norbaya Binti Yahaya

Date : ……..

DECLARATION OF STUDENT

I declare that this research entitle **"Factors Influencing Employee Behaviour towards Information System Security (ISS) in the Organizations"** is the result of my own research except as cited in the references. The research has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : …….

Name : …….

Date : …….

DEDICATION

I would like to dedicate my work to my family, friends and not forget to my supervisor for the guidance and helped me prepared this work.

ACKNOWLEDGEMENT

I would like to express my gratitude and appreciation to all that gave me the possibility to complete this report. A special thanks to my beloved and dedicated supervisor Dr. Nusaibah Binti Mansor who always provided me advice, the material and help me to coordinate my research especially in writing my report.

Besides that, I also want to express my deepest thanks to my parents Sarbanon binti Ali and Md Suffian bin Md Yunas who always motivated me along this research journey. I also would like to thanks to my fellow friends Nurul Amalina binti Sarwe, Nurul Ajmal binti Mohd Shukri, Nur Nazatul Shasha binti Mazlan and Muhammad Zakwan Zayani binti Zawawi for supported me to complete this research.

This appreciation goes to all those people who participated directly or indirectly helping me so that my undergraduate research can be accomplished on the stipulated time. Hopefully, in future, this research will be references and direction to other students.

ABSTRACT

Nowadays the Internet has become one of the fundamental aspects of the organization. It is the same as electricity. Without it, the companies or organization cannot operate well or cannot function at all because of the threat. Same goes to the information system without the security the organization are exposed to the threat. Thus, it will expose the company information to their competitors. The threat not only come from the external user but also internal user especially from the end user. Information system security (ISS) is important for both private and government organization to protect the data to keep it confidential, available and assuring its availability. However, ISS cannot depend heavily on technology. Even more, attention should be given to the behavioural views of users with regard to the security of information. In this study, the researchers have proposed a framework regarding the factors influencing employees' behaviour towards ISS in an organization. The factors influencing employee behaviour towards ISS in this study are from the individual factor (attitude, self-efficacy, and cues to action) and organization factor (organizational culture, information security policy, training and awareness). This research is using explanatory study which can help to explain the relationship between variables. Besides that, this research is quantitative research where the sources of information are gathered from the questionnaire towards 200 respondent. Primary and secondary data are chosen as a data collection method. The finding shows, the most significant factors influencing employee behaviour towards ISS in the organization is the attitude. Other than that, this research also provides the suggestions of strategy that can apply in the organization to improve their ISS regarding employee's behaviour.

ABSTRAK

Pada masa kini Internet telah menjadi salah satu aspek asas organisasi. Ia sama dengan elektrik. Tanpa itu, syarikat atau organisasi tidak boleh beroperasi dengan baik atau tidak boleh berfungsi sama sekali kerana ancaman tersebut. Begitu juga dengan sistem maklumat tanpa keselamatan organisasi terdedah kepada ancaman. Oleh itu, ia akan mendedahkan maklumat syarikat kepada pesaing mereka. Ancaman bukan sahaja datang dari pengguna luaran tetapi juga pengguna dalaman terutama dari pengguna akhir. Keselamatan sistem maklumat (ISS) adalah penting bagi organisasi swasta dan kerajaan untuk melindungi data untuk memastikan ia sulit, tersedia dan memastikan ketersediaannya. Walau bagaimanapun, ISS tidak boleh bergantung sepenuhnya pada teknologi. Lebih-lebih lagi, perhatian harus diberikan kepada pandangan tingkah laku pengguna berkenaan dengan keselamatan maklumat. Dalam kajian ini, penyelidik telah mencadangkan rangka kerja mengenai faktor-faktor yang mempengaruhi tingkah laku pekerja terhadap ISS dalam organisasi. Faktor-faktor yang mempengaruhi tingkah laku pekerja terhadap ISS dalam kajian ini adalah dari faktor individu (sikap, keberkesanan diri, dan isyarat untuk bertindak) dan faktor organisasi (budaya organisasi, dasar keselamatan maklumat, latihan dan kesedaran). Kajian ini menggunakan kajian penjelas yang boleh membantu menjelaskan hubungan antara pembolehubah. Selain itu, kajian ini adalah penyelidikan kuantitatif di mana sumber maklumat dikumpulkan dari soal selidik kepada 200 responden. Data primer dan sekunder dipilih sebagai kaedah pengumpulan data. Dapatan menunjukkan, faktor yang paling penting yang mempengaruhi tingkah laku pekerja terhadap ISS dalam organisasi adalah sikap. Selain itu, penyelidikan ini juga menyediakan saran strategi yang boleh digunakan dalam organisasi untuk meningkatkan ISS mereka mengenai tingkah laku pekerja.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

The rapid development of this era has brought about the rapid change especially in the organization. The use of Information Systems (IS) has been used in every organization to facilitate all matters. The competitiveness of most companies all around the world depends on the efficiency of using information technologies and IS particularly. IS the main objective is to provide the right people with the right information at the right time. Besides that, it has been used to track, store, manipulate and distribute the information gathered data to appropriate persons when necessary. Retrieving, processing, storing and distributing data to support organizational decision-making and control are interconnected IS components (Gupta & Saini, 2013).

As organizations become increasingly dependent on strategic advantages and operations on IS, IS safety issues are also increasingly important (Kankanhalli, et al., 2003). As such, Information Systems Security (ISS) ensures that business or company information is kept safe. The ISS refers to the process and methodology involved by storing confidential information, available, and ensuring integrity. Additionally, ISS is very important as it refers to access control, which prevents unauthorized personnel from entering or accessing the system, protecting information no matter where such information is in transit as in an E-mail or in storage areas. In addition, the ISS also works to detect and restore security breaches, and document the events.

However, no matter how to advance the technology is, the ISS of the company it still cannot depend heavily on that technology only. The success or failure of IS

depends on the practices behaviours of IS by end users. Yet more attention should be given to the behavioural views that will influence the users with regard to IS. For example, Predd, et al., (2008) stated that several users habitually decide to break these policies as they want to speed up their work or increase their own efficiency. Besides that, the careless of employee that doing mistakes accidentally also can breach the information of the organization such as accidental employee data sharing or confidential data transmission without proper encryption. According to Cheng, et al., (2017), malicious employees can bypass all company security policies by disguising sensitive information and threatening to send it via encrypted or covert channels to normal documents.

Security issues could be caused by users insecure behaviour when the workers using an IS. The employee behaviour towards ISS will give positive impact if they follow the policies but on the other side, the negative behaviour will crucial to the companies or the organization. In this regard, expert trust that information security technological aspects cannot only assure a safe and secure environment and also that the behaviour of human information security must be taken into consideration (Furnell & Nathan, 2012).

1.2 Problem Statement

In this highly competitive world, the IS has become the backbone of not only success but the survival of organizations in this highly competitive world. As organization are increasingly dependent on IS for strategic advantage and operations, ISS issues are also becoming much more important (Kankanhalli, et al., 2003). In addition, CyberSecurity Malaysia stated that the exposure to cyber threats is higher now, as almost all organizations in the private and public sectors are increasingly dependent on information and communication technology for their operations and services (New Straits Times, 2016).

According to these matters, organizations focus and take action for managing threats to their ISS by securing their network using anti-virus/ anti-spyware, firewalls, interruption detection and prevention systems and content filtering software. However, this technical defence layer for the security of an organization can surrender to human failure (Suk Rhee, et al., 2009). There may also be a risk for careless or uninformed employees. For example, guessable password on vulnerable accounts or account is logged in when nobody uses the device and error such as submitting a document to the wrong address could also be destructive to organizations. Winkler & Hayden (2005) stated that users often disclose their passwords and e-mail the company's directory or other sensitive and classified information by manipulating social engineering. From that matters, an estimate indicates that more than half of all security breaches are caused by the careless behaviour of social engineering and end users (Mackezie, 2006).

Hence the behaviour of workers towards ISS is very important to enhance the privacy of the company. According to Safa, et al., (2016), Information Security conscious care behaviour decreases the risk of information breaches when the area of weakness is human behaviour. Negligent of employees is a key threat to IS security (Siponen, et al., 2006). The irresponsible of the employees is a key threat to ISS. Security issues could be caused by user's unsecured behaviour when they are using an information system. Users of ISS issues related behaviour are so various and complex that they can hardly be defined by a unified explanation. One important reason is that the context where users engage in behaviour vary (Yang Li, 2015).

Besides that, information systems are often exposed to different types of threats. This threats cause different types of damages and could lead to financial losses. The damage to information security may include everything from financial losses to collapse of an entire information system. Employee's failure or action can lead to these threats. In response to this problem, the aim of this research is to identify the several factors that influencing employee behaviour towards ISS in the organization. This is because employees are the end users of the company. Besides that, the employee will give a threat to the organization if they cannot control their behaviour very well. Thus, the factors that will be influencing employee behaviour should be focused to enhance and sustain the ISS in the organization.

1.3 Research Question

The research questions are:

i. What is the factors influence employee behaviour towards ISS in the organization?
ii. What is the most significant factor that influencing employee behaviour towards ISS in the organization?
iii. What is the strategy that can be suggested to the organization in ISS in companies

1.4 Research Objective

The objectives of the research question are:

i. To determine the factors influence employee behaviour towards ISS in the organization.
ii. To analyze the most significant factor that influencing employee behaviour towards ISS in the organization.
iii. To suggest a strategy to organizations in ISS in companies.

1.5 Scope of the Study

The research will be conducted for the private and government organizations in Melaka Tengah. The research was using questionnaire and data collection technique as the research method. Target respondents of the questionnaire are the employees that work in private and government organization as they were occupied with the information system in their company in the matter of using the system at the company. The data collection will support the research. The result of the research will be used for further research objective.

1.6 Limitation of the Study

The limitations of the research are more on the human factor. Due to the large scale of the questionnaire, there was a lack of accuracy in answering the questionnaires as the human error will appear. As the respondents were selected at random to perform the research, the honesty level of respondents was different from each other. So, there was a limitation to the validity of the result got from respondents. The awareness of risk towards information system security in companies among the respondents too was affected the validity of the research as not everyone was aware of the importance and the impact of information system security of the company. Besides that, the researcher also faces the limitation of time regarding data collection.

1.7 Significance of the Study

The importance of this study was to determine the factors that influencing employee towards ISS in the organization. By having to know about the factors that influencing employee's behaviour on ISS it will help the future researcher to study about employee behaviour on ISS. Besides that, from this research organization can be executed or modified for a better ISS. Indirectly, this research created a strategy for the organization on the security of IS for the employee in the workplace. For the organization that are applied IS, this research will contribute to the selection of choosing the best way to know about the most significant factors of employee behaviour towards their ISS in the organization. As a consequence, the organization can develop an effective security strategy or program for a secure environment.

1.8 Summary

In this chapter is an introduction of what the research is all about. Here, the researcher stated the problem statement about the factor that will impact the organization. Besides that, the researcher also lists all the research objective and research question that want to study in this research. Other than that, the scope and limitation of this research also stated by the researcher. Lastly, the importance of this research according to factors influencing employee behaviour towards ISS in the organization are also recognized in this chapter.

LITERATURE REVIEW

CHAPTER 2

2.1 Introduction

This chapter will discuss more in the literature review for this research. The factors that influencing employee behaviours towards ISS in the workplace were discussed in this chapter. The theory for the overall chapter will make the researcher be able to construct the theoretical framework which will summarize this chapter. The researcher has focused on what factors influencing employee behaviour towards ISS.

2.2 Employee Behaviour Definition

The term of employee behaviour relates to how well employees react to specific working conditions or situations. Though many elements determine the behaviour of an individual in the organization, employees are influenced by the organization culture and also their culture itself. The employee itself and also the organizational culture influence the way employees interact with each other and also their management. Moreover, the trusts of an employee influence his or her ethics and sense of ethical responsibility. According to Pattinson, et al., (2015), human beings pose a significant threat to the security of the computer systems of an organization and to the information they process and store. So this perception refers to the behaviour of employees who often "operate" a computer that may range from accidental to malicious occurrences to irresponsible actions.

However, to identify the causes of employee behaviour is not an easy task. The factors that contribute to any behaviour are varied, complicated and hard to determine

(Werner & DeSimone, 2012). So that, in this research the researcher has select several factors as independent variable and categories it in two factors that influencing employees behaviour which is individual factors (attitudes, self-efficacy and cues to action) and organizational factors (information security policy, training and awareness, organizational culture). This is because the researcher wants to know either all these factors will influencing employees behaviour towards ISS in the organization.

2.3 Information System Security Definition

The ISS is the hardware, operating systems and application software used to process and store data for organizations to create a safe environment (Kim & Solomon, 2016). Today, organizations conduct business with collaboration through the telecommunications network in a global multi-enterprise environment, particularly the Internet. So, it is important to make sure all the data are being secured. So, it is important to make sure all the data are being secured.

In the development of high technology nowadays, most of the organizations are depending on the ISS. This is because, for today's business advancement, the information between employees is moving quickly and threats can come from almost anywhere. Because of that, the information should be safeguarded from damage done by threats that lead to loss, unavailability, modification and incorrect admission. According to Saleh, et al., (2011), attacks involve mistakes and oversights, deception, accidents and deliberate changes. Gupta & Saini (2013) stated that the requirements of secure information can be satisfied if the organization can make it confidentiality (information can only be viewed by authorized users), integrity (information can be changed only by authorized users) and availability (information available to authorized users when requesting information). Thereby, IS is a fundamental element of information technology control.

2.4 Protection Motivation Theory

In this research, the researcher has looked into the Protection Motivation Theory (PMT) as a basis for this research. This research builds a new framework for looking at the factors that influencing employee behaviours. Thus, this guiding framework is used to address the research question presented in Chapter One which is what factors that influencing employee behaviour towards Information System Security in the organization.

The theory of motivation for protection was specifically evolved to examine how fear influenced users to change behaviours in their health (Rogers, 1983). Then in the context of information security, an employee within that organization is likely to feel some effects if the organization is affected by a threat. The concepts highlighted in the PMT and in the literature on fear appeals can, therefore, be applied and are relevant in the context of information security (Herath & Rao, 2009).

Thus the coping assessment, which involves reaction efficiency and self-efficacy, focuses on adaptive responses. It determines a person's ability to deal with a threat and take action to prevent it (Rajendran & Shenbagaraman, 2016). The self-efficacy has a positive effect on security policy attitude (Rajendran & Shenbagaraman, 2016).

Next the figure 2.1 shows the Protection Motivation Theory:

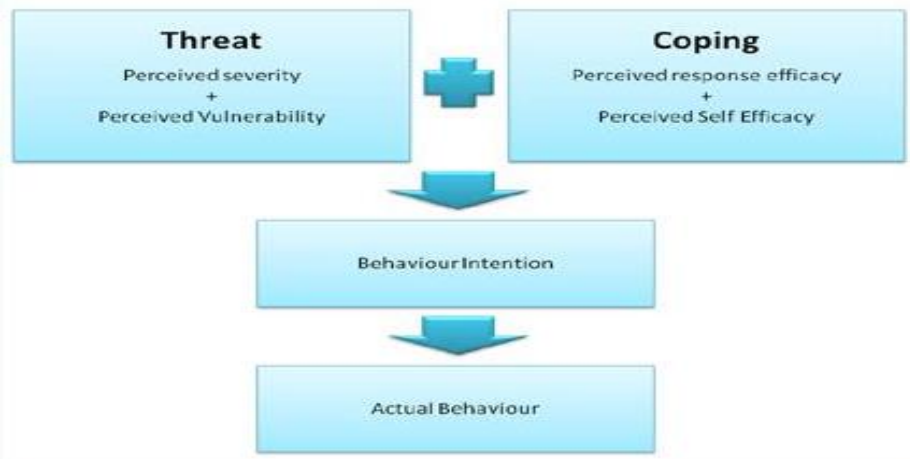

Figure 2.1: Protection Motivation Theory

There are several previous findings of PMT. According to Anderson & Agarwal, et al., (2010), PMT was one of the most powerful theories to determine the desire or intention of users to take protective action. Besides that, PMT delivers a theoretical explanation which really can explain why people take those certain countermeasures to investigate potential threats to computers, which ultimately prevent frequent attacks upon computer systems (Crossler, 2009). Other than that, PMT was applied to many computer security technology research projects and was used in studies on the intention of users to use security software to protect against the threat of spyware (Johnston & Warkentin, 2010). Safa, et al., (2015), use PMT to study user behaviour in a way that minimizes the risk of infringement of information security. The assessment of IS and self-efficacy are two main factors in PMT; the results of data analysis in the previous study confirmed that threat assessment and self-efficacy have a significant effect on the conscious behaviour of information security.

For this research, PMT theory has helped the researcher to identify the factors that influencing employee behaviour to make sure the ISS in the company become safer before anything bad happens and affects the organization especially in determines a person's ability to deal with a threat and to take measures to avoid it.

2.5 Factors Influencing Employee Behaviour towards Information System Security

In this research the researcher are focusing on factors influencing employee behavior from main factor which is individual factor (attitude, self-efficacy, and cues to action) and organization factor (organizational culture, information security policy, and training and awareness). Both factors will explain below: