CHAPTER I

INTRODUCTION

1.1 Introduction

With the advancement of technology, higher education institutes face challenges to secure their information assets that could be vulnerable to breach of security. Information security issues are considered the top priorities in various organisations including those in academic sector. Computer security and crime are considered serious and challenging issues to information system, protecting the assets of the information depends on the success of the information security plan and the execution of various security controls within the organisation (Alshamrani & Mehdim, 2012; Ahlan & Lubis, 2011).

In general, there is a considerable reliance on the human element in the field of information security in terms of behaviour and knowledge; this means that people who are engaged in work associated with information security must possess the necessary knowledge about protecting information and ensuring a high level of security of information (Kruger et al., 2011).

Information security issues were investigated as a technical problem for many years, without paying attention to the human factor and how security culture and awareness of information security affect users' behaviour in providing additional protection for information assets (Alfawaz et al., 2010).

In recent years, with the increasing needs for information security systems, many studies indicated that security applications and software could not provide the required security level to information systems. Moreover, many scholars found that information security systems need extra dimensions beyond technical level such as human behaviour, organisational values, cultural beliefs, awareness, experience and practice. These can be created by organisation's members and could significantly contribute to information system security (Wang & Zeng, 2010; Malcolmson, 2009; Rotvold, 2008).

Information security awareness minimizes the level of risks to information assets, specifically by reducing the risk of employee unwise behaviour and harmful interaction with information assets. With the rise of mobility and the effect of globalization, modern organisations require guidance in establishing information security aware or implementing an appropriately stringent information security culture (O'Brien et al., 2013). Therefore, the risk can be caused by the employees themselves regarding the security of information assets because of weak practicing and unawareness of information threats (Da Veiga & Eloff, 2010).

It becomes essential to protect information assets from internal threats. However, the threat of the human element in the information systems is considered

more important issue in information security. Researches reveal that unintentional security incidents from the insiders often occur, which could cause great devastation to information assets more than outsider attacks. In addition, researchers found that the majority of threats to an organisation' information system can be attributed to the weak experience and the awareness level of employees of how to deal with the internal and external security attacks to information assets (Parsons et al, 2014; Roy, 2010; Colwill, 2009).

1.2 Background of the Study

The development of Information and Communication Technologies (ICTs) is becoming very common throughout society. Therefore, it is a must to protect information assets, but information cannot be protected by technical means solely, information security currently extends to include the values and awareness of user towards information security. Information security is one of the important issues discussed in Institutes of Higher Learning (IHLs); the development of information systems is accompanied with developing new ways to attack these systems (Ismail et al., 2010).

According to the survey on the security incidents and attacks conducted by MYCERT, Cybersecurity Malaysia for the quarter (Q1) in 2015, from January to March 2015 MYCERT, reported a total of 2909 incidents, about 2190 incidents were reported, the most categories of incidents includes spam, intrusion attempt, denial of service vulnerability report, fraud, cyber harassment, content related, malicious codes and intrusion (MYCERT, 2015).

It is evident that information system security practices encompass both technical and non-technical issues to protect organisational assets from a variety of information system threats (Ismail et al., 2010). Therefore, training programs are necessary for university employees to gain a better experience to seal with information threats, and providing organisation's information security policy will contribute to protect information assets (Rezgui & Marks, 2008).

Several studies indicated that information security incident is due to the fact that users lack of information security knowledge. Therefore, users must engage in education and training programs that directly promote security awareness, as well as, organisations should provide these programs to achieve foreseeable results from enforcing security policy (Williams & Ayobami, 2013; Kritzinger & von Solms, 2010).

Moreover, employees need to be educated on information security issues to protect their information systems from security threats (e.g. external and internal attack). In addition to that, investigating information security awareness among employees will reduce the rate of insider threats in organisations (Guo, 2013; Kruger & Kearney, 2006; Wilson & Hash, 2003). Organisational management has become more focused on the security policies and security awareness training of employees to assist protecting information system, understanding the relevance and effect of policy, behaviour, training, education, and knowledge of technology on the security awareness of employees is necessary to determine the role of these factors on the overall security of an organisation (Fakeh et al., 2012).

Based on the above statement, any wrong behaviour or inappropriate act by an employee in using information systems without considering the security measures in the work environment has a negative effect on information security and could present a big threat to information system and cause a loss of confidential information belong to students in the educational institutes hands of attackers of the information system. As a result, some controls are needed to be in place to secure the information system (Gupta & Sharman, 2012; Scarfone et al., 2008; Allen & Westby, 2007; Guttman & Roback, 1995).

Several organisations provide information security awareness programs and training on information security to increase the practices of employees to ensure they acquire adequate knowledge of information security risks. Therefore, it is evident that assessing the information security awareness within organisations aims to steer the interaction and security practices of employees concerning information systems and contribute to the protection of information assets (Talib et al., 2010).

Increasing the awareness towards information security and increasing the level of experience of training employees is critical to protect information assets of organisations. Previous experience offers the user a unique perspective associated with information security; users who know more about internet security techniques are likely to be more aware of internet security threats (Jaw & Chen, 2007).

This study relies on (Ismail et al., 2010) study which revealed that over 95% of departments in Malaysian universities have a high level of technological implementation, but 54% were failing poorly on organisational measures, especially

with lack of security procedures, administrative tools and awareness creation activities. The finding indicates that the culture in information security is very weak in Malaysian universities. In addition to that, information security threat has been reported to be on increase among users of internet technologies, especially the academic communities, comprising the students, lecturers and tutors.

1.3 Problem Statement

Information security is considered a challenging issue for organisations, especially the academic ones to secure their information. Further, Higher Education Institutions (HEIs) encounter various security threats resulted from advanced and complex attack methods due to insufficient current security practices, in addition to the technological aspect, implementing and imposing appropriate policies and procedures in compliance with security policy and regulation is considered a prerequisite to secure information assets from security threats (Ismail et al., 2010).

Employees in organisations and who are also home users of computing technology are susceptible to security breaches unless they comply with the organisation policy to use safeguards such as firewalls and antivirus programs. Colleges and universities may be easily exposed to attacks by hackers for two reasons: the first reason is the open access provided by the university for students and guests while the second reason is the role of the staff and employees in protecting information systems within their organisations as classified information still possesses real concern for organisations (Ishak et al., 2014; Rezgui & Marks, 2008; Hazari et al., 2008).

The Use of technology is mainly in two locations which are workplace and home. Many programs and initiatives were proposed to improve security awareness among users, most of these initiatives are directed towards organisations while some national programs are directed to home users, this interprets that education about information security occurred more in the workplace rather than the home environment. Few research studies focused on staff security awareness both in workplace and home so there is a strong need to investigate security awareness in these two areas (Talib et al., 2012).

In this study, the problem is to identify the effect of policy, behaviour, training, knowledge of IT, and education on employees' security awareness and practice level both in workplace and home.

1.4 Motivation of Study

According to the study conducted at USIM by Halim et al., (2008) to evaluate information security awareness and practices among the staff; the research found that there are a number of security issues where the respondents general attitudes were "very positive" but they do not believe that these "positive things" are being practiced in their organisation, such as, they believe that in general all attachments to e-mail should be scanned for a virus, but they do not believe that this practice is applied in their organisation, as well as, the study considered any negative practices by employees as follow:

- Writing passwords on post- it notes.
- Leaving computers on without protection.
- Open unexpected email attachments.
- Soliciting weak passwords.

The study focused on academic staff only which is considered not enough to measure the security awareness and practices among USIM staff, as the administrator's staff plays a primary role in protecting information assets where they interact with the information assets of the organisation more than the academic staff. In addition, the sample size of 43 respondents is considered very limited that cannot provide a clear evaluation of security awareness and practices among staff.

An effective information security management requires a great understanding of both technological and human dimensions of the supervisors and management staff (Talib, 2012; Ahlan & Lubis, 2011). However, there is an essential requirement to provide consultation regarding security issues and to increase awareness of security problems and threats among employees working in educational institutes in Malaysia. For security awareness to succeed, it needs a foundation of security policies.

Security awareness is an important concept that must be instilled in employees through assorted ways. Recently, many organisations focus on implementing security policies and security awareness training programs to educate their employees on the importance of information security. These programs can increase employees security awareness as well as, other factors can also affect employees' security awareness level, such as policy, behaviour, education and knowledge of technology beside the training

(Fakeh et al., 2012). This research proposed to contribute to the literature by identifying and evaluating the effect of policy, behaviour, training, knowledge of IT and education on the security awareness and practices of USIM employees both in workplace and home.

1.5 Research Questions and Hypothesis

1. How the factors of policy, behaviour, training, knowledge of technology and education might influence the security awareness and practice in both workplace and home?

2. What is the current awareness and practice level of information security among the employees in USIM?

The following research hypotheses have been formulated and tested to answer the questions stated above.

Hypothesis 1:

H1a: Policy has a positive effect on security awareness and practice at workplace.

H1b: Policy has a positive effect on security awareness and practice at home.

Hypothesis 2:

H2a: Behaviour has a positive effect on security awareness and practice at workplace.

H2b: Behaviour has a positive effect on security awareness and practice at home.

Hypothesis 3:

H3a: Training has a positive effect on security awareness and practice at workplace.

H3b: Training has a positive effect on security awareness and practice at home.

Hypothesis 4:

H4a: Knowledge of Technology has a positive effect on security awareness and practice at workplace.

H4b: Knowledge of Technology has a positive effect on security awareness and practice at home.

Hypothesis 5:

H5a: Education has a positive effect on security awareness and practice at workplace.

H5b: Education has a positive effect on security awareness and practice at home.

1.6 Research Objectives

This research works on the following objectives, as stated below:

1. To investigate the effect of policy, behaviour, training, knowledge of technology and education on information security awareness and practice both in workplace and home.

2. To investigate the awareness and practice level of information security among the employees of USIM based on the identified factors.

1.7 Methodology

The methodology that used in this research presented in Table 1.

Table1: Summary of Methodology

Research Questions	Research Objectives	Approach	Data Collection	Expected Outcome
Q1: How the factors of policy, behaviour, training, knowledge of technology and education might influence the security awareness and practice in both workplace and home?	**1:** To investigate the effect of policy, behaviour, training, knowledge of technology and education on information security awareness and practice for both workplace and home	Quantitative	Questionnaire	Significant of investigated factors
Q2: What is the current awareness and practice level of information security among the employees in USIM?	**2:** To investigate the awareness and practice level of information security among the employees in USIM based on the identified factors.	Quantitative	Questionnaire	Report related to the level of awareness and practice

1.8 Research Scope

The scope of this study is to evaluate the security awareness and practice among academic and administrative staff, and their ability to practices security of information assets in the workplace and home. However, the present study is limited to investigating security awareness and practice in Universiti Sains Islam Malaysia (USIM), whereas further investigation is required in other Malaysian universities to extend the knowledge of information security.

1.9 Significance of the Study

The main significance of this study is based on developing the awareness of human factor on the safety of information systems, and understanding the effect of policy, behaviour, training, knowledge of IT and education, on the security awareness and practice of employees in both workplace and home in USIM, to reduce the risk resulting from a lack of security awareness which leads to protect information assets, where security awareness and practice has a significant effect to address the various human factors that can cause damage to the security of information.

To that end, previous literatures have been reviewed either conceptually, and empirically concerning some related factors to information security threat generally, with few (if at all any) studied information security awareness' relationship within the conceptual framework of community training, vulnerability to threats, perceived threat severity and compliance to security policies with the information security threat. This research study will contribute in analysing the factors of policy, behaviour, training,

knowledge of IT, education, and its effect on employee security awareness and practice in both workplace and home. The importance of this research stems from its contribution to the following aspects:

1. Knowledge Outcomes

Five factors that affect security awareness and practice of employees in both workplace and home were determined that are; policy, behaviour, training, knowledge of technology and education, these factors will be used in this study to evaluate the security awareness and practice in both workplace and home, so the area of application of the model is extended to cover the home also.

2. Security Outcome

Discussion of the proposed model contributes to understand and enhance the knowledge on information security awareness and practice for employees in both workplace and home this will help educational organisations to implement an information security awareness that protect the confidential information of students and organisation from many kinds of security threats that can causes loss or any damage by attackers that may lead to financial loss.

1.10 Research Publications

The following paper was produced to disseminate some concepts and results from the work that has done by the author during the course of this research study:

- Asker, H. O. & Jali, M. Z. 2014. "A Comparative Study on the Information Security Culture Related to Workplace and Home Practices". *Proc. Of the Second Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2014. Copyright © Institute of Research Engineers and Doctors, USA. 22nd/Dec/2014. ISBN: 978-1-63248-034-7 doi: 10.15224/ 978-1-63248-034-7-33*

- Asker, H. O. & Jali, M. Z. 2015. "A Comparative Study on the Information Security Culture Related to Workplace and Home Practices". *International Journal of Advances in Computer Networks and Its Security– IJCNS Volume 5: Issue 1 [ISSN : 2250-3757]. Publication Date: 30 April, 2015*

1.11 Thesis Outline

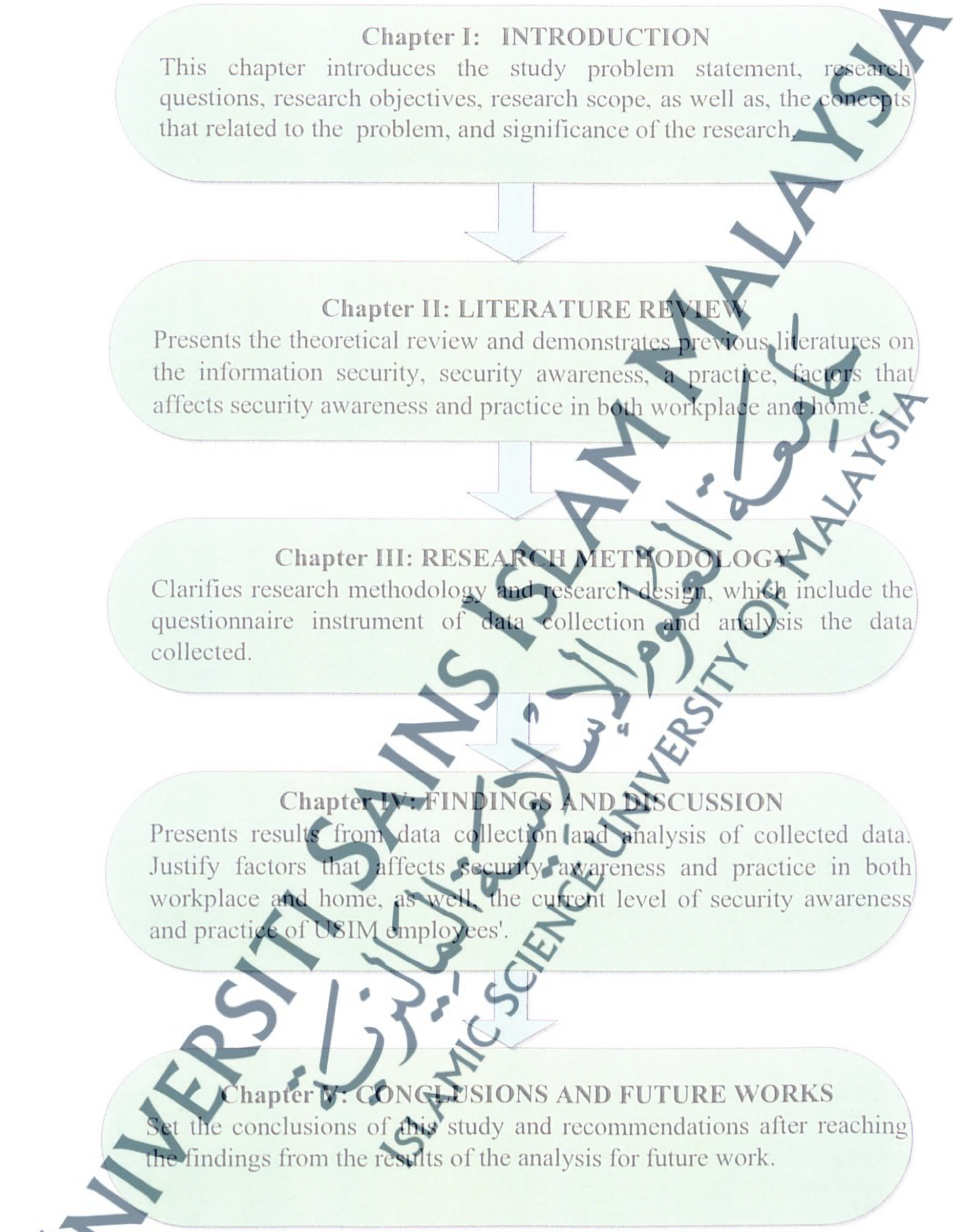

Figure 1: Descriptive Outline of Thesis