# CHAPTER 1

# INTRODUCTION

## 1.1 Introduction

The significance of information for organizations has increased. Organizations nowadays depend to a large extent on Information Systems (IS) for their daily operation (Bulgurcu et al., 2010; Whitman & Mattered, 2011; Wybourne et al., 2009). In fact, organizations may suffer strategic, operational as well as financial setbacks when facing any threat or damage to information (Alhogail & Mirza, 2014; Crossler et al., 2013; Wybourne et al., 2009). This is why most organizations give high priority to managing information security (Bulgurcu et al., 2010). Information security is described by Whitman & Mattord (2013) as "protecting information and its critical features (integrity, confidentiality and availability), as well as the systems and hardware that preserve, utilize and transfer that information, by implementing policy, technology and training and awareness programs". Furthermore, according to Herath & Rao (2009), there are three components that determine the effectiveness of information security in organizations, i.e., people, process and technology.

It is the individuals that use technology; therefore, every security system should essentially be based on the human factor and invest in the individuals using the systems because they are the insiders of an organization (Soltanmohammadi et al, 2013). Insiders are typically trusted and have complete access to the organizational Information System. Due to the privileges granted to them, they can carry out crimes within their workplace without leaving any proof (Colwill, 2009; Grimes, 2010; Warkentin & Willison, 2009). Insiders are able to make a significant impact without leaving any evidence to be identified, which is what makes malicious insiders

extremely dangerous (Colwill, 2009; Fernando & Yukawa, 2013; Grimes, 2010). It is asserted by Colwill (2009) that the key factors of any insider attack are typically motivation, capability and opportunity. Thus, it is vital for organizations to comprehend these factors so that they can avoid any possible threats. Typically, motivations emerge from within the individual, whereas it is the organizations that provide opportunity and capability.

The key reasons for most of the information security violations by humans are negligence, mistakes and carelessness of employees (Bulgurcu et al., 2010; Herath & Rao, 2009; Safa et al., 2015; Warkentin & Willison, 2009). According to a few security studies, IS may experience greater damages due to unintentional security behaviour rather than intentional security behaviour (Abdul Molok et al., 2010; Colwill, 2009; Fernando & Yukawa, 2013; Liu et al., 2009; Loch et al., 1992). It is easy to repeat unintended security incidents for employees' convenience, but organizations are unable to detect it till the damage has been experienced (Fernando & Yukawa, 2013; Guo et al, 2011; Herath & Rao, 2009; Liu et al., 2009). Colwill (2009) stated in this regard that the security incidents will keep occurring till the insiders continue to have the authority to access the organizational IS. The defence mechanism would not be able to accomplish the organizational goal of securing their information systems (IS) even when the organization has a sophisticated defence system if its insiders are exhibiting improper behaviour (Rupere et al, 2012). Though the technical control mechanisms can automate various security controls, these mechanisms are unable to regulate the behaviour of certain employees; thus, other methods of control are required, e.g., education and security measures. An important point to note is that every end-user system function cannot be automated (Herath & Rao, 2009).

Carstens et al (2004) presented the following effects of human errors in information security: disruption in information system, integrity of information being compromised, dissemination of incorrect or confidential information, huge economic loss, services not being delivered adequately and reputation being adversely affected. There are several ways in which the Unintentional Insider Threat (UIT) can occur, for example, sensitive information may be sent to unauthorized people through mail, email or fax, or becoming a victim of social engineering (Forcepoint, 2016). For instance, a person working in the immigration department in Australia sent an email to the organizer of the Asian cup soccer tournament by mistake that included passport and visa information of President Obama and 30 other world leaders participating in the Group of 20 summit in Australia (Phillip, 2015). Krebs (2015) mentioned another example, where an American organization released credit card details of 25,000 of their customers. This happened because hackers used the username and password of a district manager to access the information system (IS) of the company as the manager had his username and password mentioned on the front of his laptop.

To ensure information security, organizations mostly rely on entirely technical-based solutions (Bulgurcu et al., 2010; Fernando & Yukawa, 2013; Ifinedo, 2014). However, since information security involves "technical issue", "people issue" as well as "organizational issue", technical solutions are not sufficient on their own to secure organizations from threats (Bulgurcu et al., 2010; Ifinedo, 2014; Workmaet al, 2008). Therefore, a comprehensive approach needs to be developed by organizations that includes people, process and technology so as to secure there IS assets (AlHogail, 2015; Furnell & Thomson, 2009; Ifinedo, 2014). In fact, it is preferred that organizations should concentrate more on humans because process and technical

control systems should be consistent with the security functions of the employees (Bulgurcu et al., 2010; Fernando & Yukawa, 2013).

Therefore, the main focus of this study is to present the unintentional insider threats countermeasures model that describes mitigation measure in three areas of UIT countermeasures, i.e., human factor's countermeasures, organizational countermeasures and automated defence tools countermeasures. Automated tools alone are insufficient to protect and prevent insider threats. Thus, this study presents the development of Unintentional Insider Threats Countermeasure Model (UITCM) that is based on mixed approaches which can be used as countermeasures towards UITs especially in Malaysian's SMEs. The model is further been evaluated by using expert-based judgement through Delphi method with the aim to reach acceptable level of agreement among experts and remove any uncertainty in the model. It is hoped that, the model may help in formulating the information security policy of the organization and the information security awareness program to overcome the unintentional insider threats.

### 1.2 Problem Statement

Several organizations employ and use advanced technologies in their security systems, for example smart cards and biometrics, which is why external threats are the not the main cause for concern in information security. Rather, the main risks emerge from the errors, carelessness and omissions of the users that are brought about when the users act inappropriately (Kreicberga, 2010; Leach, 2003, Hughes-Lartey et al., 2021). In various security breaches caused by the employees of an organization, external cybercriminals are given access intentionally or unintentionally (Kreicberga, 2010; Siponen et al., 2010; Mazzarol et al., 2021). The defence system of an

organization would not be able to secure the information system if despite having a sophisticated defence system, its insiders' exhibit improper behaviour (Rupere et al., 2012). Humans are responsible for most of the security incidents occurring. Thus, it is ultimately humans that cause harm to the system and it is not possible to fully avoid human errors. Furthermore, human errors were found to be the main security threat in organizations (Loch et al., 1992; Whitman, 2004; Abu-Musa, 2006; Mazzarol et al., 2021). The greatest insider threat of all is UITs (Trzeciak & Costa, 2014; Rupere et al, 2012). UITs remain an increasing cause for concern for public and private organizations and denote a significant risk for business (Mazzarol et al, 2021; Alsowail & Al-Shehari, 2021; Mazzarolo & Jurcut, 2020). Automating security controls and using information security technologies does not always bring about an increase in security (Whitman, 2004; Bulgurcu, 2008; Rupere et al., 2012; Herath & Rao, 2009; Mazzarolo & Jurcut, 2020; Bean, 2006; Mazzarol et al, 2021).

There is very limited literature on insider threats in Malaysia (Isnin & Sedek, 2018); however, various cases regarding human negligence have been reported. For instance, it was deduced in the studies by (Samy et al, 2010; Humaidi & Balakrishnan, 2013) that a significant internal threat in Health Information Systems in Malaysia is human error.

Asai & Perez (2012) performed surveys in nine investee countries and deduced that US-based companies situated in Malaysia are likely to face greater risks because employees share confidential information unintentionally. Humans impose the following challenges in implementing cyber security in Malaysian organizations in the public sector: inadequate skills among the staff, human error and lack of accountability to cybersecurity (Khalid,2020; Samy et al., 2021). The highest percentage of security breaches due to human errors was recorded in Italy and

ASEAN (IBM, 2020). The key threat agents in higher education in Malaysia include malware, social engineering attacks, intrusion and human errors and unintended disclosures (Ulven, 2021). The factors behind the main ICT security threats to data centers in the public sector in Malaysia are direct factors which are, unprofessional staff and lack of manpower for security tasks, lack of awareness of users that lead to human errors, and indirect factors which are, inadequate budget, insufficient monitoring and compliances, inadequate security policies and process that effect the employee and therefore lead to human errors (Khalid, 2020; Samy et al., 2021).

Though efforts have been made by Malaysian government through different organizations to avoid cybercrimes and information security threats by enacting various cyber laws and policies, regulating such threats still depend on individuals (Shammugam et al., 2021). It was demonstrated in studies that the tendency of information sharing exhibiting by Malaysian employees is considered as a natural behaviour. The issue is possibly because of the high collectivism nature of the society (Asai & Waluyan, 2008; Waluyan et al., 2010; Asai & Hakizabera, 2010),and according to the findings of these studies, the "unintentional sharing of confidential information" is the most severe issue out of the various problems that foreign companies may experience in Malaysia. This is because of the local employee's belief on supporting others or "teaching others" (Waluyan et al., 2010). The second most severe issue is "lower priority to information security policy" due to the employees' perspective about rules being flexible. These study results have been examined by a few Malaysian employees and it is clear from their comments that the results are consistent with the attributes of the Malaysian society (Waluyan et al., 2010). It was shown in the findings pertaining to the degree of the likelihood of threats in the computerized banking systems in Malaysia that these systems mainly face threats

from UITs (Malami et al., 2012). It is shown in the literature that UITs are the greatest security threats faced by Malaysian organizations, and further studies need to be carried out on this issue (Malami et al., 2012; Asai & Perez, 2012; Waluyan et al., 2009). In a review carried out on insider threat status in Malaysian companies, it was shown that the most common threats are unintentional human errors or mistakes like unintentionally leaking sensitive company information on social networks (Tuor et al., 2017; Isnin & Sedek, 2018; Mazzarol et al, 2021). Malaysia is highly vulnerable to cyber-attacks, being one of the top ten countries that are vulnerable to cyber-attack in addition to the United States and North Korea (Isnin & Sedek, 2018, Mat et al., 2020). The risk of cyber-attacks is faced by 65% of the Malaysian organizations (Roy, 2010; Amiruddin, 2016; Isnin & Sedek, 2018). Over 10,000 cases and reports related to cyber-attacks and crimes are received by Cyber security Malaysia each year (Roy, 2010; CyberSecurity Malaysia, 2021). The threats are faced from various areas, for example human, system, technology, etc. However, the issue mainly stems from the humans themselves (Roy, 2010; Hughes-Lartey et al., 2021). Insider threats and risks related to it are not unique and strange for Malaysian organizations. However, majority of these organizations decide not to challenge the risk openly. They are not willing to discuss their experiences and challenges regarding handling the issues associated with insider threats, which is possibly because of their fear of acquiring a negative reputation. These incidents could cause reputation loss for the organizations (Apau et al., 2018).

Various aspects need to be taken into account to avoid, identify and respond to an incident. At present, the preventive measures being used are entirely based on technical approaches and are not adequate; insider threats cannot be managed with technology alone (Stahie, 2019; Ivan et al., 2018). To decrease the risk of

unintentional insider threat, multi-layered defensive approaches need to be enforced by organizations, comprising of policies, processes, awareness, technical control and being attentive to sociological and psychological areas (Friedlander 2016; Saxena et al.,2020; Mazzarol et al., 2021; Omar, 2015; Soomro et al., 2016). The Malaysian government have set numerous cyber laws and regulations to prevent cybercrimes and information security threats but so far there are few laws and regulations dedicated to control human threats.Control of such threats in Malaysian organizations still dependent on the people (Shammugam et al., 2021; Mazzarol et al, 2021).

The existing UITs countermeasures were reviewed, and it was found that the prevailing countermeasures are not adequate. Each existing countermeasure that was reviewed dealt with one aspect or a few aspects of human errors. All of the countermeasures were not completely covered in all aspects of human UIT errors. Brown's solutions to human error were condemned by Rupere et al. (2012) as the errors should be anticipated before they took place. The technological, human and organizational factors are not considered in the SOP and trust model. Furthermore, Gonzalez and Sawicka framework (Rupere et al, 2012) and Trcˇek and Kandus model (Rupere et al, 2012) are quite theoretical. The security issues are not clearly identified in the Model of Saha and Misra (Rupere et al., 2012). Gonzales & Sawicka (2002) assert that automation will not be able to solve the issue of human error. Though UIT Mitigation Strategies presented by (Ismail & Yusof,2019) and UIT Mitigation Strategies by Greitzer et al. (2014) were quite comprehensive and covered the problem aspects, they did not include a few vital areas like design of work setting, instrumental conditioning, design of user-system interfaces, stimulation of risk perception, trust model, incident-driven reviews to policies, practices and training materials and sometimes, re-evaluate risk completely. Human error should be

addressed using a comprehensive approach that consists of different aspects. This is where the existing models are inadequate, which is why UIT cases continue to increase. This indicates the shortcoming of the current approaches to solve the UIT issue.

Thus, the aim of this research project is to formulate a conceptual model by examining the current models and countermeasures recognized in the literatures, including the vital organizational, technological and human factors to decrease the unintentional insider threats. In this research, SMEs in Malaysia were used as a case study to identify issues of UIT in Malaysian context.

### 1.3 Research Questions

This study focuses on to the following research questions:

A. What are the contributing factors of the unintentional insider threats in Malaysian's SMEs?

B. How to incorporate the countermeasures of the identified factors into an unintentional insider threats (UIT) countermeasures model?

C. How to evaluate the validity of the proposed model to be used in Malaysian's SMEs?

### 1.4 Research Objectives

The research aim is to mitigate the UITs by presenting a model as a countermeasure. Three key objectives have been determined to accomplish this research aim, which are:

A. To identify the contributing factors of the unintentional insider threats in Malaysian's SMEs.

B. To propose a conceptual model for the unintentional insider threats countermeasures based on the contributing factors been identified.

C. To evaluate the theoretical validity, usability, readability and understandability of the proposed model in Malaysian's SMEs by using expert-based judgement through Delphi method.

## 1.5 Research Scope

This research focuses on identifying the contributing factors and the likelihood level of UITs in an organization by using SMEs in Malaysia as a case study. A survey was conducted towards the IT Executives in SMEs companies. The participants in this research are 311 IT Executives from 311 SMEs from technology MSC companies listed under InfoTech. The online survey was conducted and quantitative and qualitative methods were used to achieve the objectives of the study.

At the end of the research, a conceptual model as a countermeasure towards unintentional insider threats is developed. The countermeasures model is based on the existing countermeasures in the literatures with an additional input based on experts' suggestion during model evaluation. The model was evaluated by experts' review through two rounds Delphi method to evaluate the theoretical validity, usability, readability and understandability of the proposed model. Delphi method is used to reach acceptable level of agreement among experts and remove any uncertainty in the model. The experts were selected based on their experience in the study area that represents the theorists (academicians) and professionals (practitioners) from different international and local academic institutions and cybersecurity industry. Qualitative approach was employed for the descriptive analysis of the features of the respondents' profile and the first round of Delphi evaluation. While, quantitative approach was

employed for the likelihood and contributing factors of UIT and the second round of Delphi evaluation.

### 1.6 Thesis Structure

To fulfil the intended aims of this study, every chapter is structured such that it fulfils one or more objectives. The background of the issue, the study objectives, research questions and the scope of the study were presented in Chapter 1. An extensive review of the related literature and the studies that backed the current study were presented in Chapter 2. The research methodology and measurement used in the research were discussed in Chapter 3. Chapter 4 discussed the initial version of UITCM which developed based on the literature review of existing countermeasure to formulating a conceptual model that serves as a countermeasure towards UITs. To develop the second version of UITCM a survey was conducted towards IT Executives of Malaysian SMEs, to identify factors and likelihood of UITs in Malaysian SMEs.

This study identified the likelihood of UITs to justify the need for the proposed model and examined whether the study problem still existed by identifying the likelihood of UITs. The most contributing factors of UITs have been identified in order to give them more focus and concern during the model development process and to ensure that they covered from all its aspects. The questionnaire of this study serves as a roadmap for developing the proposed model by determining of how much the need for the model, as well as identifying the most contributing factors of UITs to be fully covered. Then, the primary validating procedure of the proposed model (UITCM) was done as the last step of the development procedure. The primary validating is based on a literatures and existing models analysis. Validation of the final

version of the model was made by expert validation. In Chapter 5, the conclusion and recommendations for the study findings were presented.

## 1.7 Summary

This chapter aims to present the introduction of the study, the research problem, research questions, research objectives and the scope of the study. Finally, the overall structure of the thesis was presented. In the next chapter, the foundation of the study will be explained by presenting detailed knowledge on unintentional insider threats of organization information security.