CHAPTER II

LITERATURE REVIEW

2.1 Introduction

This chapter presents theoretical background related to the context of this research. The discussion is concentrated to provide a foundation for the inquests of the principal research questions to this research by reviewing the literature relating to the concepts of information security. The chapter is organized as follows; section 1.1 introduction, section 2.2 definition of terms. Section 2.3 discusses a comprehensive review of information security studies involving section 2.3.1 information security. Section 2.3.2 security awareness, section 2.3.3 security practice, section 2.3.4 information security and workplace users, information security and home user section 2.3.5, security awareness and practice at home and work place section 2.3.6. Section 2.4 factors that effect information security awareness and practice. This pillar is structured to study the proposed model of the factors that affect security awareness in both workplace and home. Section 2.6 presented the conceptual framework for the security awareness and practice. The road map of this chapter is summarized in Figure 2.

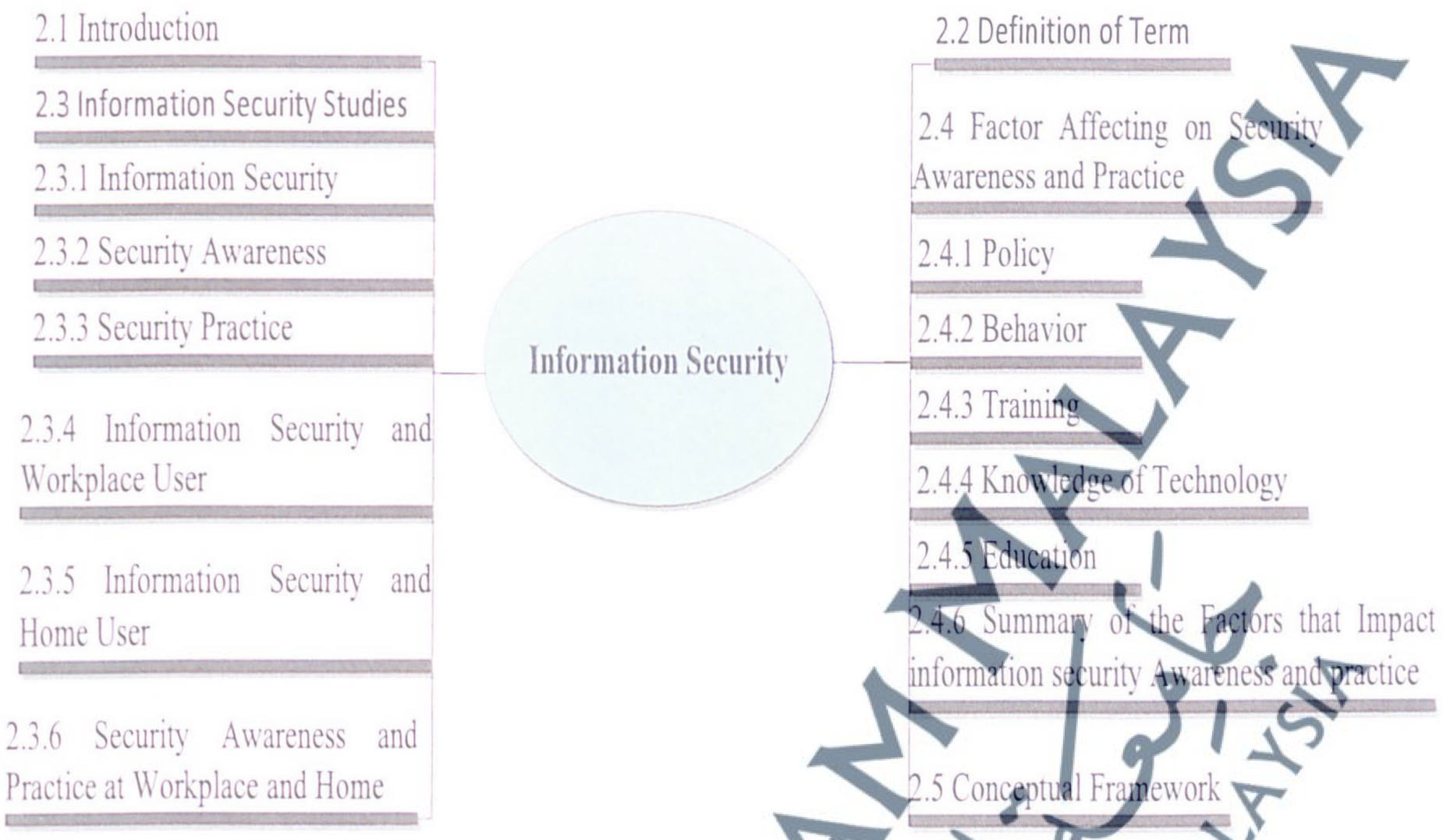

Figure 2: Chapter two road map

2.2 Definition of Terms

This section demonstrates the keywords that are used throughout this research study, the definitions of these keywords help the reader to understand concepts mentioned in this research study. The following are the keywords in this research:

- **Information Security:**

The process of preserving and protecting information assets, information systems and hardware from unauthorized uses, detection, modification, destruction in order to conserve confidentiality, integrity, and availability of information and information systems (Hussein et al., 2011).

- **Security awareness:**

Security awareness means that the employees in organisations are aware and understand the significance of information security, policies and compliance with security procedure to protect their information assets (Siponen, 2000). Within the context of this thesis security awareness is also referred as information security awareness.

- **Security practice:**

Security practice is a start point to measure user`s behaviours on information security to provide metrics to evaluate the investment in information security training and awareness program (Montesdioca & Maçada, 2015).

- **Information assets:**

Consists of information, data, knowledge or experiences that could be monetary, operational and scientific information, organisations, students and employees, information assets have significant value to stakeholder (Bryniolfsson, 1994).

- **Home users:**

Home user is a citizen who uses Information Communication Technologies (ICTs) for personal use anywhere outside their work environments, also he accesses the Internet from a personal computer at home, as well, he is self-responsible to secure his computer in terms of malware, updates, patches (Kritzinger & Von Solms, 2010).

- **Workplace users:**

Workplace users are those users accessing the Internet from their corporate work stations within their work environments such as industry areas, government areas, and academic areas. Those users use ICTs under security policies and regulations of information security in their organisations (Kritzinger & Von Solms, 2010).

2.3 Information Security Studies

This section discusses the previous literature in information security, information security and home users, information security and work place users, security awareness and practice at home and work place, and factors affecting information security awareness and practice.

2.3.1 Information Security

Information security is the process of protecting information that has a recognized value; the information is the core of information security that must to be protected. The information security involves all the technical, behavioural, managerial and organisational approach to reduce the threats on information assets. The aim of information security is to ensure the Confidentiality, Integrity and Availability (CIA) of information assets of an organisation (Bozic, 2012; Albrechtsen, 2007; Da Veiga et al., 2007).

Information security is one of the significant issues that have been discussed. For instance, in Institutes of Higher Learning (IHLs) in Malaysia, securing information is significant in protecting the organisation information assets and reducing the security threats. Studies reported that IHLs have faced several security incidents on their information resources, such as, information security breach, hacker gain access to faculty member's names and social security numbers (Ishak et al., 2014; Kvavik & Voloudakis, 2003).

Several studies emphasized the effect of human factor on the information security, the human factor has a formidable influence on the success and failure of the organisation's efforts to secure and protect their services and information system. The end-user is still the weakest link on the information security, the information security is not solely a technological issue, but, the users issue also; an information security is the most important requirement in the working day of employees and employers (Metalidou et al., 2014; Kreicberga, 2010).

Information security threats have experienced a significant evolution in terms of volume and nature, shifting from technical savvy hackers with unerring skills to organize and meticulous crackers aiming to gain financial benefits for their work (Talib et al., 2010). The increasing threats of information systems brought new solutions that focus on the technological means; while the researches that focused on the human factors are limited; hence researchers have called for more examination in this area (Metalidou et al., 2014).

According to Jones et al., (2010) organisations thought that insiders are the essential fraction of the losses of the organisation's information systems, where 69% of the respondents reflected the financial losses to insiders. The majority of the security incidents were caused by unintentional mistakes by employees, the majority of respondents reflected that the security incidents are stemming from misuse of network resources. Consequently, cybercrime activities have increased and end-users find themselves the recipient of threats.

According to Richardson et al., (2008) more than half (52%) of firms have been threatened in 2007 alone, while 64% of the study respondents admitted to encounter phishing email, a threat that was not widespread 5 years ago. In this regard, user's protection has been proposed in a range of security countermeasures. These safeguarding tools constantly involve in terms of sophistication and in number to encounter the evolving threats as well as, depending on their effective deployment, configuration and operation by end-users.

More importantly, it is a well-known fact that the strength of security is only as effective as its weakest link, and the latter is, more often than not, the end user (Schneier, 2011). In an attempt to counter the threat experienced by end-users, increasing concentration has been directed towards information security awareness, education and information dissemination.

2.3.2 Security Awareness

According to Information Security Forum (ISF) security awareness is defined as the extent to which organisations members understand the role of information security in the protection of organisation information assets, as well as, the level of security required by the organisation and how employees understood their security policies, procedures, and practices, in order to make sure that the employees can make right judgments if they face a potential security issue (Ahlan et al., 2011; Information Security Forum, 2003).

Information security awareness plays an important role in the information security process of any organisation. In some cases, security awareness focuses on the IT department only without attentions to the employee's role in the security chain, the employees have been identified as a significant part enabling information security in the organisations, as most security incidents resulted from employees' lack of awareness about the security policies in their organisations (Alnatheer et al., 2012; Rezgui & Marks, 2008).

Information security issues are the most priorities to various institutions, as it is strongly related to the concept of risk. Although most of the organisations have implemented security technology properly, but still the risk is there due to the security attacks, such as social engineering, dishonesty and negligence and many other threats that cause losses of information in computer systems (Fakeh et al., 2012).

Information security awareness has been used in organisations to promote information security culture by increasing the employees' knowledge on information security. Several organisations instituted information security awareness programs to ensure that their employees are aware of security threats (Kruger & Kearney, 2006). Both academic and commercial communities have given attention to information security awareness in the past few years. Organisations are increasingly acknowledging the significance of their information assets and the development of effective strategies to enhance awareness within the company. This has been further supported by effective corporate governance regulation and legislation (Von Solms et al., 2006).

In information security awareness and training, Sabbagh et al., (2012) suggested that promoting security awareness and training through the curriculum in the education is suitable for all learning styles, and the main aim is to provide a platform to promote and develop security awareness and learning. The benefit from the training is to promote the knowledge of security in to security incidents, manage staff compliance with security policies in organisations. The results show that the security awareness can play an important role in the security field of education as it can be combined in different ways to deliver the information required to fit the different learning styles audience.

Ishak et al., (2014) conducted a study on information security awareness and practice among faculty staffs in University Selangor Malaysia, the study found that more than half of staff were aware of information security issues, however, they usually do not practice secure computing behaviour's. The study suggests that Malaysian IHLs should developed information security policy to confirm that academic staff can understand their role on information security at their academic institutions, security policies should be focused on security standard, password management, back-up data, comply with good security practice.

In the context of the organisation, efforts have been expanded towards enhancing awareness among workers (Richardson, 2008). As evidenced by the fact that, 82% of enterprise firms provide training. This scenario is however not common for all companies, as in the majority of small-to-medium companies only 40% reported to provide training. Few organisations possess the training resources. Even if they intend to provide training but they only constitute 95% of internet users. The

remaining 5% are home-users or the general public. The concern lies on the fact that 95% of users are prone to threats and attacks (Kritzinger & Von Solms, 2010).

2.3.3 Security Practice

Successful security practices require support of management that defines strategy to implement effective security practices in their organisation to protect information assets. Information security represents considerable concern of organisational management. Security solutions depend on the technical aspects as well as, on appropriate user behaviour (Montesdioca & Maçada, 2015).

Information systems provide important benefits to organisations, especially when the user is able to use all system capabilities. However, users may face difficulty of understanding and executing information security practices that are regulated by organisation security policy (Goel & Chengalur, 2010). The user satisfaction with information security practices and understanding the factors that affect the information security practice could help organisation to improve information systems functionality, as well as, improve information security system (Montesdioca & Maçada, 2015).

Woodhouse (2007) focused on the end user behaviour and corporate culture on information security as the low level of information security culture in the organisations and the threat that may occur in information systems are due to a result of wrongful conduct. The aim of the study was to develop a strategy to ameliorate information security culture within the organisation, by evaluating information

security practices where 16% of males and 15% of females have ability to share their own password with others. The culture within the organisation allows this behaviour, around 36% of the participants said that they use pieces of paper to keep their password on the desk, while 31% of the participants answered, they use the similar password for many times. This finding clarifies the bad security practices, the importance of security culture is to enhance human behaviour as a significant factor to secure (ISMS) from insider threats by encouraging security best practices.

According to a survey on the security perception of beginner users of the internet in UK, 43% of participants did not understand the threats, where 38% of the participants did not know how to use security packages, while, 35% of them did not know how to protect their computers. With the increase number of internet users, the attention to information security awareness and practices have become widely where it covers end users at organisations, as well as, users at home. Furthermore, organisations increase their defines by providing security awareness and practices while the home users left as attractive targets for hackers (Ishak et al., 2014; Furnell & Evangelatos, 2007).

The success of information security depends on a suitable information security practice by the end users, the weakness in user security practices constitutes a larger threat to an organisation's security more than any weakness in information security, therefore, the biggest challenge in information security are to transform users from the weakest line to the defence line by enhancing security practices (Rhee et al., 2009). According to Huang et al., (2011), the users could be the biggest vulnerability in information systems security, even with several security methods. These methods

depend on how the user using them, many studies focus on different angles that can encourage users to follow information security practices.

Rhee et al., (2009) conducted a study on the influence of self-efficacy in information security by focusing on the user information security practices, the findings reveal that users understanding of the importance of information security practices, as well, the awareness program and the education of user on security practices required during the use of organisational information systems can promote organisations' security, as well as, can be the initial key to reduce security incidents.

2.3.4 Information Security and Workplace Users

According to Chan et al., (2005) large number of information security breaches in the workplace resulted from employees' failure to comply with organisational information security guidelines. They found that 78% of computer attacks appear in the form of viruses embedded in email attachments. Employees who open e-mail attachments from unknown sources face risk infecting their own computers as well as other computers sharing the same network. Therefore, more attention needs to be paid learning how non-compliant behaviour takes place so that appropriate measures for curbing the occurrence of such behaviour can be found.

Albrechtsen (2007) explored the users' experience of information security and their personal role in the information security work. The main patterns of the study were: (1) users state to be motivated for information security work, but do not perform many individual security actions; (2) high information security workload creates a

conflict of interest between functionality and information security; and (3) documented requirements of expected information security behaviour and general awareness campaigns have little effect on user behaviour and awareness. Moreover, the author claimed that the users are considering the user-involving approach to be much more effective for influencing user awareness and behaviour.

Chan et al., (2005) examined employees' behaviour with regards to their compliance with information security. They employed the concept of information security climate and examined its mediating effect between the organisation's characteristics and employees' behaviour. They found that the climate perspective has credence indicating an alternative framework upon which employee behaviour in organisations can be studied.

2.3.5 Information Security and Home Users

Several initiatives and strategies were proposed to ameliorate information security awareness for end users; most of the initiatives were focused on organisations users, while, a few initiatives were directed to home users (Talib et al., 2010; Kritzinger & Von Solms, 2010; Furnell & Evangelatos, 2007). Home users are prone specifically to be targeted by cyber criminals due to many factors such as, home users are not aware of the risks and threats of using internet, 95% of home users accounts were exposed to internet attacks, one out of 600 (PDF) files that users download from internet contains of malicious software. This reveals that novice users are more likely to face internet security threats due to the lack of security awareness in recognizing the threats and understanding the required protection. The study proposed the e-

awareness model that consists of e-awareness portal, and the enforcement component, to improve security awareness of home users through acquaint home users on risks that they could be facing on internet (Kritzinger & Von Solms, 2010).

In their study, Furnell & Evangelatos, (2007) presented important reasons and factors that can make home users more prone to exposure to computer attacks and threats. For instance, by targeting the users that do not have any security awareness about the security risks; they are easy exposed to online scam, as the attackers have realized that it is easier to attacking home users, therefore, we should educate home user on information security awareness. Unlike organisation, home users lack the understanding of the significance of security awareness and lack the fiscal resources that are required to provide security awareness programs.

2.3.6 Security Awareness and Practice at Workplace and Home

Security awareness can be defined as ensuring that the employees are aware about the rules and security policies of their organisation, therefore, information security could be defined as the process to improve user's behaviour towards information security practices by changing behaviour or enhancing good security practices (Talib et al., 2012; Ahlan et al., 2011). With regards to home users, awareness raising initiatives has been proposed for instance, U.K. government sponsored initiative (Get Safe Online) campaign that offers general information concerning risks and protection from threats. Such initiative offers information from guidelines for particular information concerning threats and is primarily text based information coupled with a few video files (Iles, 2014; Bada & Sasse, 2014).

The U.S. and other countries also have a similar national-based websites catering to awareness. Several companies are providing security software, operating systems and web-based access and reading-based resources to educate and inform home users. Evidently, it is a challenging step to motivate home users to employ security measures as security; despite it is requirement that is not always the user's primary task. People often fail to understand that they need to follow security measures and those who do understand, have limited time to do that. According to evidence, even when users think that they are well-informed about security and self-protection, they often fall off the mark; this vulnerability is due to the lack of knowledge and awareness to protect themselves (Kritzinger & Von Solms, 2010).

According to (Chen et al., 2008; Cone et al., 2007) 75% of home users think they are protected from spam, but in reality only 42% are truly protected. This gap between what they know and the actual reality demonstrates a significant gap in understanding. Good security awareness has been investigated by various studies in a hope to create learning mechanisms like face-to-face training sessions, email messages, online training, video game, and intranet-based access and poster campaigns. Studies are primarily concentrated on what and how to educate workers in the organisation and highlighted the significance of measuring security programs effectiveness to guarantee education results in practice.

Talib et al., (2010) identified that the majority of the learning about information security occurred in the workplace where clear motivations such as legislation and regulation existed. The findings also indicated that users were more than willing to engage with such awareness raising initiatives. From a comparison of

practice between work and home environments, it was found that the knowledge and practice obtained in the workplace transferred to the home environment. By giving this positive transferability of knowledge and the willingness to learn about how to remain secure, an opportunity exists to move away from specific organisational awareness programs and to move towards awareness raising strategies, whilst deployed in the organisation, will develop an all-round individual security culture for users regardless of the environment where they are operating.

Tsohou et al., (2008) identified the ambiguous aspects of current security awareness approaches and the proposed classification provides a guide to identify the range of options available to researchers and practitioners when they design their research and practice on information security awareness. On the other hand, home users have various resources to enhance their online threat awareness and they are provided with supporting information, anti-virus providers, operating system vendors, and government initiatives Talib et al., (2010).

Despite the available training programs and initiatives at the workplace and at home respectively, research was dedicated to understand what is being relayed and where, the strategy's effectiveness and the level of learning styles' role in realizing good information security practice is still few and far between. In this regard, security awareness can be viewed from various directions like within a school, government-sponsored initiatives and security providers. In addition, a considerable amount of studies has called for the need to develop an information security culture in the organisation and to shift from surface learning to embedding good practice among workers (Furnell & Thomson, 2009; Schlienger & Teufel, 2003).

Researchers are convinced that establishing such culture in the organisation, can lead to the maintenance of long-term security practice and promote awareness and education of security issues as it facilitates employee engagement of the practice. Based on the above review, it was clear that most of the researchers focus on security awareness on one aspect, workplace users or home users, workplace users are more likely to increase their security awareness as most organisations provide security awareness programs.

2.4 Factors Affecting Information Security Awareness

In this section, a discussion is employed about the factors that influence the information security awareness and practice. These factors are grouped in Table 2.

2.4.1 Policy

Ensuring the security of organisations information assets has become more complex and challenging with the development of technology. This is a significant concern for knowledge-intensive organisations, such as universities. In addition, the effective manner of their primaries teaching and research activities depends on the availability and integrity of computer information resources. One of the most significant mechanisms that help to secure organisational information assets is through the formulation and application of information security policy. Security policy is the basis of any security system by defining the strategies of an organisation's information security approach through a written document, indicating overall policies of the

organisation: the policy aims to define employee's prerogatives and responsibilities in an organisation (Doherty et al., 2009).

More specifically, the security policy should define the organisation's approach to manage information security by determining employee's responsibilities, authorized and unauthorized uses of the system, providing tools for employees to report threats to the system, specifying punishments for violations, and defining the mechanism for updating the policy (Alnatheer et al., 2012; Doherty et al., 2009).

According to Siponen et al., (2014) the main threats to information security occur due to employees who do not comply with their organisation's security policy. The study shows that the employees, awareness, beliefs, attitudes, and social norms have important and positive effects on employees toward complying with security policies. Moreover, employees should be educated and trained on information security policy which will increase the employees' awareness on information security threats.

According to Bulgurcu et al., (2010) information security program should include all the factors that promote employees to comply with security policy such as beliefs which show positive attitudes towards security policy. Furthermore, the study suggested that information security awareness is influenced by employees' compliance with security policy, thus designing training and security awareness programs that ensure employee's compliance toward security policy will produce a security awareness culture within the organisation.

2.4.2 Behaviour

Several studies in information security linked the information security incidents in the organisations with the employee behaviour, which is resulted from a lack of security awareness in their organisations (Guo, 2013; Lim et al., 2009). According to Hussein et al., (2011) in the United States from 2005 to 2007, 277 reported breaches were noted at colleges and universities while, in 2008, there were 263 reported privacy data breaches, most breaches occurred in the academic sector.

Vroom & Von Solms (2004) discussed the importance of employee behaviour in the success of the information security system in organisations, through the exploration of the potential problems of employee behaviour on information security by presenting a detailed study about the importance of studying the employees' behaviour and organisational culture at one time, to identify the negative aspects that affect the information security of the organisation and, by changing the security culture within the organisation that would be an important factor for the integration of the culture of security in the daily conduct of the employee.

Schlesinger & Teufel (2003) focused on the massive dependence on information processing and the increase of organisational risk which became the victim of computer misuse, and by focusing on organisational culture, how it can be used to implement information security culture which aims to reduce the threats to information assets. Moreover, the aim of security culture is to influence employees' behaviour towards security policy.

The importance of human factor in computer security has been presented by (Parsons et al., 2010). Their study focused on the effect of human behaviour on providing secure information systems. The authors presented the effect of individual differences, cognitive abilities, appreciation of risk and personality traits on the behaviour of the organisations' employees that affect the information security awareness. The study suggests that security and flexibility are two factors that users need in information systems. However, the best way to improve information security is by improving all information security aspects starting with technical means, information security awareness, security behaviour of employees, and establishing security policy in organisations.

Soltan mohammadi et al., (2013) presented the human behaviour factor in their study, the study focused on the effect of human factors on information security system for health care industry in Malaysia. According to this study, some researches in Malaysia supported the importance of human security behaviour error as an internal threat in health information system in Malaysia. The internal threats caused by carelessness, error and misuses of human linked to users lack to security awareness that can address the users security behaviours.

Grant (2010) presented a study on the relationship between security awareness and the security behaviour of individuals through evaluating the security behaviour and practices of faculty and staff at Armstrong Atlantic State University to find if the staff are performing the simple security practices and behaviour every day to reduce insider threats, where, human behaviour varies among individuals, where, user's behaviour can influenced by demographic groups. The findings reveal that there is a

relation between respondents' security behaviours and their information security awareness level. The success of security in the organisation relies on the behaviour of employees who administrate and maintain information resource, a suitable and constructive behaviour of employees and system administrators can promote the efficacy of information security.

2.4.3 Training

Endeavor of security awareness is to change behaviour, as well as, promote good security practices of users by entrenching the principle of responsibility in employees about their role in protecting information assets. Security training is an essential factor to improve security awareness as a continual process that assists to identify security problems. Training aims to take out the security skills and efficiency in practitioner to construct knowledge and skill that assist in reducing security incidents in the organisations (Wilson & Hash, 2003).

According to (Tsohou et al., 2010; Schultz, 2004) security training is a continuing process and a significant factor to improve security awareness for an organisation by increasing employees security awareness, as well as, to comprehend security problems and to confirm that employees are aware about the threats and how to protect their information assets. Prior researches have shown that implementing awareness training program improves security effectiveness. Training frequency, training method, and training compliance monitoring are all mentioned in the body of literature as they playing a role in security awareness training effectiveness (Quagliata, 2010).

According to (Metalidou et al., 2014) offering training is one of the factors that increase employees' level of satisfaction. However, employees' training on security risks and measures against attacks should be conducted carefully. According to (Bada & Sasse, 2014) training program is significant for disseminating security awareness to users to do their jobs.

2.4.4 Knowledge of Technology

Knowledge and skills enhance people's ability to meet their needs, extend the variety of available options in all areas of their lives. The skills people possess can also enhance their sense of self-worth, security and belonging (Zanoon& Gharaibeh, 2013). Nowadays, access to information and proficiency with technology are becoming more important. An inclusive society will increasingly require everybody to have high levels of knowledge and skills.

Also, knowledge of technology is important, as information is organized and communication by using technology so knowledge can change human behaviour. By having knowledge, users can act appropriately as they know how to act when something occurs, by making the right decision for a situation, and in the exact time to avoid inappropriate events in the workplace, such as, knowledge of specific technologies that relate to their security and privacy when using the internet, can avoid harm from happening (Fakeh et al., 2012).

Furthermore, (Zanoon & Gharaibeh, 2013) investigated the effect of customer knowledge on security of E-business and discussed some security gaps, which resulted

from the low level of customer knowledge in information technology. Most of the organisations depend on information technology in their work, such as managing records, technology helps to facilitate daily work, as information is organized by using technology. Knowledge can alter human behaviour and users can behave appropriately when something occurs for information security system (Fakeh et al., 2012).

2.4.5 Education

Education level merges all security skills and efficiencies from different specializations into the common source of knowledge; in addition, it also provides a foundation of concepts, issues, and principles that produce IT security professionals (Wilson & Hash, 2003). According to Payne (2003), technology alone cannot solve security concerns; therefore, the universities must apply an overall plan for security that includes specified technical approaches, policy development, efficient education and awareness programs as a way to professional development for all employees which ultimately assists in reducing new threats as well to avoid security incidents in universities.

Hight (2005) presented security education, training and awareness (SETA) program which is an educational program designed to develop security awareness of employees to reduce the security violations that refer to deficiency security awareness of employees. The SETA program could be considered as portion of risk management, which determines the security tone for the employees by keeping security as a daily activity in their work.

Several studies indicate the necessity of promoting information security education to motivate employee information security awareness, applying security education is significant for organisation's security management practices. Education can affect the knowledge of employees while information security education for employees can be applied through campaigns, briefings, discussions, speeches, and seminars that increase information security in an organisation (Fakeh et al., 2012; Takemura, 2010; Hight, 2005).

2.4.6 Summary of the Factors that Affect Information Security Awareness and Practice

Consequently, from the effect of training in security awareness perspective, Quagliata (2010) attempted to examine the patterns of association between training frequency, training method, and training compliance monitoring variables and security effectiveness. The findings indicate that training method and training compliance monitoring have a strong relationship with perceived security effectiveness, whereas training frequency does not.

In their study, Kruger et al., (2011) examined the effect of culture factors on human factors, they indicated that the cultural factors do play an important role in security awareness levels for students. According to (Kaur & Mustafa, 2013), information security awareness of employees indicates attitude and behaviour that are found to be significantly influence (CIA) of business information. The security awareness is a very important factor that is used in establishing the security effectiveness as mentioned by Shahri et al., (2013).

Moreover, from behaviour perspective, Chou (2013) explored the influence of personality and organisational citizenship behaviour on information security awareness. The results showed that most of the respondents are classified as goal orientation traits, a higher level of organisational citizenship behaviour, and information security with a high level of awareness. The personal attributes of each variable showed inconsistent relationships. Personality has positively associated with organisational citizenship behaviour variable and every dimension of information security awareness.

Darvishi (2013) investigated the components that are affecting information security behaviour in enhancing awareness and designed an information security behaviour model to enhance awareness. They found a significant relationship between self-efficacy, security practice-care behaviour and intention to practice privacy protection on information security awareness behaviour. One different study grouped the factors based on institutional factors.

Haeussinger & Kranz (2013) investigated the mediating effect of security awareness among individual and environmental factors. Their findings showed that providing employees with comprehensible and readily accessible information security policy provision and improving employees' IT knowledge are the two most influential factors on information security awareness.

Fakeh et al., (2012) examined the information security awareness among academic librarians, the study found that four key factors that have influence information security awareness among the staff that are policy, behaviour, knowledge

of IT, and education. Policy provides the rules, regulations, and objectives regarding information security. Therefore, constructing and implementing policy within organisations ensures that information can be protected. Education can influence employees' security awareness through educating employees during seminars, awareness programs, training, and campaigns. Knowledge of IT is also important in order to avoid misuse of IT devices, which leads to lack of information security. Finally, employee behaviour is interrelated with awareness of information security in the workplace. Good behaviour towards information security practices can also influence information security.

Table 2: Factors Affect the Information Security Awareness

Authors	Factors		
	Independent Variables (IV)	Mediator	Dependent Variable (DV)
(Quagliata, 2010)	• Training frequency • Training method • Training compliance monitoring		• Perceived security effectiveness
(Kruger et al., 2011)	Cultural factors • Beliefs • Values and assumptions		Human factors • Knowledge • Behaviour
(Fakeh et al., 2012)	• Policy • Education • Behaviour • Knowledge of technology		• Awareness
(Chou, 2013)	• Personality • organisational citizenship behaviour		• Information Security Awareness
(Darvishi, 2013)	• Privacy policy (PP) • Self-efficacy (SE) • Security practice care behaviour (SPCB) • Intention to practice privacy protection • Security practice technology (SPT)		• Information Security Awareness
(Kaur & Mustafa, 2013)	• Knowledge. • Attitude • Behaviour		• Information Security Awareness
(Shahri et al., 2013)	• Security Awareness • Security culture		• Security Effectiveness
(Haeussinger & Kranz, 2013)	Institutional factors • Information Security Policy Provision. • SETA Programs. Individual factors • IS Knowledge • Negative Experience Environmental factors • secondary Sources' Influence • Peer Behaviour	Information Security Awareness	• Intentions to Comply

2.5 Conceptual Framework

Figure 3: A conceptual framework for the security awareness and practice

Table 3: Sources of constructs taken from the previous researches.

Construct	Sources
Policy	(Fakeh et al., 2012)
Behaviour	(Fakeh et al., 2012; Haeussinger & Kranz, 2013; Kaur & Mustafa, 2013; Kruger et al., 2011)
Training	(Haeussinger & Kranz, 2013; Quagliata, 2010)
Knowledge of technology	(Fakeh et al., 2012; Haeussinger & Kranz, 2013; Kaur & Mustafa, 2013; Kruger et al., 2011)
Education	(Fakeh et al., 2012)

2.5.1 Research Hypothesis

Table 4: Proposed Hypothesis

Variable	Hypothesis
Policy	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.
Behaviour	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.
Training	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.
Knowledge of Technology	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.
Education	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.

2.6 Summary

In summarizing the above literature, to ensure that information security could be achieved in any organisation, there is a sufficient review of literature to warrant research into the proposed key factors that affect security awareness and practice of employees in both workplace and home. Several studies on information security

awareness and practice presented these factors and their role on the security awareness and practice and their various roles on the information security within an organisation. These key factors are: policy, behaviour, training, knowledge of technology, and education. The conceptual framework for the security awareness and practice and hypothesis present the relation between the factors that are identified and the security awareness and practice.

In brief, the main aim of this chapter is to highlight the existing body of literature on the topic under this study. To achieve these objectives, several definitions are explicated. In addition, some other important constructs were identified and their relationship is verified in order to provide justification and support for including them in the present study. The next chapter is research methodology, a comprehensive explanation on the research approach, method, research hypothesis, data collection, data analysis and pilot test, are presented.