AN INVESTIGATION ON THE RELATIONSHIP BETWEEN SECURITY KNOWLEDGE CONSTRUCTS AND EMPLOYEE BEHAVIOUR IN ORGANISATIONS

AMJAD ABD ALLAH MAHFUTH

COLLEGE OF GRADUATE STUDIES
UNIVERSITI TENAGA NASIONAL

2020

AN INVESTIGATION ON THE RELATIONSHIP BETWEEN SECURITY KNOWLEDGE CONSTRUCTS AND EMPLOYEE BEHAVIOUR IN ORGANISATIONS

AMJAD ABD ALLAH MAHFUTH

A Thesis Submitted to the College of Graduate Studies, Universiti Tenaga Nasional in Fulfilment of the Requirements for the Degree of

Doctor of Philosophy (Information and Communication Technology)

MARCH 2020

DECLARATION

I hereby declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently submitted for any other degree at Universiti Tenaga Nasional or at any other institutions. This thesis may be made available within the university library and may be photocopies and loaned to other libraries for the purpose of consultation.

_____________SIGN____________

Amjad A. M. Mahfuth

Date :

ABSTRACT

Many studies have revealed that organisation's insiders pose risks to the security of information assets. Nonetheless, among the major threats to a secure information environment are the actions and behaviour of the employees when handling information. Insiders, intentionally or unintentionally, can cause serious risks, despite investments usually made on security control measures and other security related products. The employee behaviour in information security cannot thoroughly be solved by technical and procedural controls alone. An organisation's approach to information security should include employee behaviour, as the organisation's success or failure effectively depends on the things that its employees do or fail to do. In order to develop appropriate security perceptions between employees within an organisation, we need to know the security knowledge required to influence employee behaviour. The literature review indicated that there is a positive relationship between knowledge and behaviour. The aim of this research is to investigate the security knowledge required to influence employee behaviour and to examine the impact of security knowledge on behaviour. This would help to guide organisations in instilling the security knowledge required in employees that would influence their behaviour when interacting with information assets in order to help minimize the internal security incidents posed by the insiders. To achieve this, the KAB (knowledge, attitude and behaviour) model has been adapted in order to investigate the relationship between knowledge and behaviour and to examine the impact of security knowledge to behaviour. This research uses a mixed method approach. The semi-structured interviews has been conducted by information security specialist to gain an in depth understanding of security knowledge constructs that are required to influence the employee behaviour in organisations. Then, a questionnaire was used to collect the data from the employees' in Palestinian healthcare services. The result of semi-structured interview analysis revealed that the six items of security knowledge constructs namely knowledge of security threat, knowledge of organisation information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility and knowledge of security risk are all relevant to help influence the employee behaviour in organisations. The result of the quantitative analysis revealed that the knowledge of security threat, knowledge of security risk, knowledge of security responsibility and knowledge of legislation, regulation and national culture have significant effect on employee behaviour. Furthermore, the result has also shown that these knowledge security construct have significant positive indirect effect on behaviour through attitudes.

ACKNOWLEDGMENT

Praise to Allah the Almighty for the blessings I have been favored in this long journey of seeking knowledge. Praise goes to Him for helping me to pass the difficulties experienced in my Ph.D. study.

I would like to express my gratitude to some people who have made significant contributions to accomplishing this work with their guidance and moral support during my PhD. I owe my deepest gratitude to them.

First, it is with immense gratitude that I acknowledge the support and help of my supervisor, Assoc. Prof. Dr. Salman Yussof who encouraged, guided and supported me from my initial step to the final step in carrying out this study. He has enabled me to develop a better understanding of the subject. The current thesis would not have been possible without her aspiring guidance, invaluably constructive criticism and friendly advice during the entire period of the study. I cannot never forget Dr. Asmidar Bte. Abu Bakar and Ass.Prof.Dr. Nor'ashikin Bte. Ali for their supervision and help to me. Also the thanks is connected to Prof. Dr. Syikin Bt Md Din for help and support to me.

I would also like to extend my thankfulness to the entire staff in College of Computing & Informatics at the Universiti Tenaga Nasional, and our research group service science members for their valuable help, support and sharing of ideas and experience in research doing. Such support has been of value for me to continue the process of research doing. Last, and the most, my sincere gratefulness and appreciation should be dedicated to all my lovely family members for their support, patience and encouragement that they have been offering me with for the long journey of my PhD. Special thanks should be expressed to my father, mother, brother, sisters, wife and children for their infinite love and caring and moral support for me during my PhD.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIC	Akaik Information Criterion
AMOS	Analysis of Moment Structures
AT	Attitudes
AVE	Average Variance Extracted
BH	Behaviour
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CR	Composite Reliability
GOF	Goodness-Of-Fit
HIS	Health Information Systems
ISA	Information Security Awareness
ISM	Information Security Management
KAB	Knowledge – Attitude – Behaviour
KLRNC	Knowledge of Legislation, regulation and National Culture
KOISS	Knowledge of Organisation Information Security Strategy
KSRK	Knowledge of Security Risk
KSRS	Knowledge of Security Responsibility
KSTG	Knowledge of Security Technology
KSTH	Knowledge of Security Threat
MLE	Maximum likelihood Estimation
NFI	Normed Fit Index
PHIC	Palestinian Health Information Center
RMSEA	Root Mean Square Error of Approximation
SEM	Structural Equation Modelling
SMEs	Small and Medium Enterprises
SPSS	Statistical Package for Social Sciences

TLI	Tucker-Lewis Index
TTAT	Technology Threat Avoidance Theory
US	United State

LIST OF PUBLICATION

1. Amjad Mahfuth, Salman Yussof, Asmidar Abu Baker, Nor'ashikin Ali, A systematic literature review: Information security culture. 2017 International Conference on Research and Innovation in Information Systems (ICRIIS). IEEE.

2. Amjad Mahfuth, Salman Yussof, Asmidar Abu Baker, Nor'ashikin Ali, A Conceptual Model for Exploring the Factors Influencing Information Security Culture. International Journal of Security and Its Applications Vol. 11, No. 5 (2017), pp.15-26 http://dx.doi.org/10.14257/ijsia.2017.10.5.02.ISSN: 1738-9976 IJSIA Copyright ⓒ 2017 SERSC Journal.

3. Amjad Mahfuth, Salman Yussof, Asmidar Abu Baker, Nor'ashikin Ali. A Systematic Review On Data Security And Patient Privacy Issues In Electronic Medical Records. Journal of Theoretical and Applied Information Technology (Scopus Indexed). The International Conference on Research and Innovation in Information Systems. Vol.90. No.2. 2015, (ICRIIS'15).

CHAPTER 1

INTRODUCTION

This chapter presents an introduction to the thesis. It first introduces the main topic, then it presents the problem statement, the research questions, the research objectives and the research scope. The chapter then proceeds by establishing the structure of the thesis.

1.1 Research Background

Information Technology has become an invaluable asset in most aspects of life, business, industries, organisations, governments and other sectors. This transformation leads to most organisations adopting the technology to perform daily tasks. Consequently, these changes have introduced a lot of risks to user and organisational information assets. Therefore, the organisations need to enhance their information security capability to protect the organisation's assets and respond to new challenges and risks to ensure the stability and continuity of the organisation.

Information security is not a purely a 'technical' issue; it is also an issue associated with 'people'. Security controls often require some form of human involvement and the humans' role is very important in the information security process (Van Niekerk & Von Solms, 2010). In most organisations, managing information security threats focuses on managing technology and process, but little efforts are made to manage people (Van Niekerk & Von Solms, 2010; Parsons et al., 2015; Von Solms & Furnell, 2016). Organisations will not be able to protect the integrity, confidentiality, and availability of information assets if they ignore the human factors.

Information is considered to be very essential for organisations to the extent that it is regarded as a key asset of a given organisation (Van Niekerk & Von Solms, 2010). Therefore, protecting this information is crucial to ensure the stability of the organisation and to maintain the availability, integrity and confidentiality of that information. A recent study by Ponemon Institute (2018) indicates that many organisations have lost billions of dollars as a result of information breaches or information violations. These breaches have also had some negative effects on customer trust. Among the major threats faced by an organisation are the employees' acts and behaviours especially when they interact with the organisation's assets. A study on the data breach investigation reports indicates that employees inside organisations could be responsible for most of the data breaches that occur, whether intentionally or unintentionally (Verizon, 2014; Internet Security Threat Report, 2018). Moreover, many studies (Božić, 2012; Da Veiga, Martins & Eloff, 2007; Da Veiga & Eloff, 2010; Schlienger & Teufel, 2003) have concluded that insiders can pose many threats to the safety of the information inside an organisation.

In information security, human error and human negligence contribute to most of the data breaches in organisations (Da Veiga & Eloff, 2010; Martins & Eloff, 2002; Schlienger & Teufel, 2003). Hence, concentrating only on technical measures to protect an organisation's assets without any consideration of the human factor is clearly inadequate (Appari & Johnson, 2010; Samy, Ahmad & Ismail, 2009). Thus, on one hand, employees play a prominent role in creating threats to an organisation and on the other hand, they can play a key role in protecting against, or preventing, such breaches. Therefore, organisations should focus on employees' behaviour, attitudes, knowledge, assumptions and awareness in order to establish an information security culture. Essentially, the effectiveness of any type of security system depends on employee's behaviour towards the organisation's information assets (Boujettif & Wang, 2010). Employee behaviour can be defined as the way of employee behaves in doing their work either in positive way or in negative way (Rashid, Zakaria, & Zulhemay, 2014). The employee behaviour in organisation may affect the organisations' information security effectiveness.

In general, most organisations have made the efforts to manage information security by focusing on the technology and process. Most organisations spend their money on technical measures and security products (Niekerk & Von Solms 2006; AlHogail & Mirza 2014). However, not many organisations spent money on the management of human behaviour in terms of providing information security between the employees (AlHogail & Berri, 2012). An organisation's approach to information security should focus on employee behaviour, as the organisation's success or failure effectively depends on the things that its employees do or fail to do.

Creating an information security culture within an organisation can reduce the harmful interaction of employees towards organisation's information assets. Furthermore, it will reduce the risk of employee misbehaviour when they interact with the organisation's assets (Van Niekerk & Von Solms, 2010; Verizon, 2014). Information security culture guides how things are done in organisation in regard to information security, with the aim of protecting the information assets and influencing employees' security behaviour (Alhogail, 2015). There are many definitions of information security culture given in the literature. Given below are two of them:

- Da Veiga & Eloff (2010:198):"*The attitudes, assumptions, beliefs, values and knowledge that employees use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour evident in the artefacts and creations that become part of the way things are done in the organisation to protect its information assets. This information security culture changes over time".*
- Alhogail & Mirza (2014:3):*"The collection of perceptions, attitudes, values, assumptions and knowledge that guide how things are done in the organisation in order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees' security behaviour in a way that preserving the information security becomes a second nature".*

The other definitions of information security culture are provided in Section 2.4.

In general, the definitions given in literature can be divided into two groups. The first group such as Alhogail & Mirza (2014, 2015); Ngo et al. (2005) define information security culture as guides that influence security behaviour. The second group such as Da Veiga & Eloff (2010); Malcolmson (2009) define information security culture as the result of security behaviour. For this thesis, the latter definition is adopted, where security behaviour will lead to information security culture after it has been practiced for a long time. This definition is chosen due to the relationship between knowledge and behaviour as described by (Zakaria, 2004; Van Niekerk & Von Solms, 2010; Al-Hogail, 2015). Knowledge and behaviour have to be integrated as significant factors in information security culture studies (Al-Hogail, 2015), knowledge directs the employees' behaviour in organisations and thus, directing the behaviour will lead to information security culture after it has been practiced for a long time. This research aims to investigate the security knowledge constructs required to influence the employee's security behaviour. This can then be used as a guide to organisations to instil the security knowledge required among the employees to influence their behaviour when interacting with information assets to minimize security risk. This relationship is further discussed by studies focused on security knowledge and behaviour in Section 2.6.3.

For further explanation, organisations' employees handle information assets during their daily work routine in the organisation. Employees (i.e. insiders) in particular feel the need to practice some security tasks so as to confirm the security of the information assets within this organisation. Consequently, when an employee has the potential to practice some of these tasks in their daily work, such tasks are supposed to be an integral component of their daily routine. Thus, these practices turn out to be common practices between the employees in this organisation and there is a good chance that the employees' behaviours will be dedicated to secure the organisation information assets. Day after day, the employees' strong commitment contributes to the objective of creating a well-established culture of information security among the employees themselves.

Therefore, it is clear that we can develop an information security culture within an organisation because it is also a learned process. The presence of an appropriate information security culture can be used as a guide to direct the employees in their learning of different information security practices, which they can later be adapted in their day to day work routines.

When all employees understand this security behaviour, they are more likely to practice it. When these practices become common, they then become a part of the daily work routine after which, as mentioned, an information security culture is ultimately developed among the employees.

In this thesis, we use the term "behaviour" to refer to "security behaviour". There are many definitions of security behaviour given in the literature. Given below are two of them. The other definitions of security behaviour are provided in Section 2.3.

- (Milne, Labrecque, & Cromer, 2009:450): “Security behaviour as specific computer-based actions that individuals take to keep their information safe, and protective security behaviours”.
- (Ng et al., 2009:817): “Security behaviour will reduce the risk and/or impact of security incidents”.

Numerous studies indicate that the user’s attitude and lack of security awareness are the most significant contributors to security incidents (Kitchenham & Charters, 2007). Such findings support the need to instil an information security culture in order to influence employees’ behaviour within organisations. Some studies such as Alhogail & Mirza (2014) & Von Solms (2006) argue that security of information can be protected and managed if an effective information security culture is taken into consideration and the employees are able to recognize, know, understand and manage their own perceptions so as to secure their organisation’s assets. The key to establishing such a culture lies in giving employees the required security knowledge and the specified skills they need to interact with the organisation’s assets. The outcomes will help to influence the employees’ behaviour and protect the organisation’s assets.

Most studies indicate that the establishment of an information security culture is very important to develop an effective information security (Da Veiga et al., 2007; Van Niekerk & Von Solms, 2010). However, such a culture must be supported by adequate knowledge regarding information security (Van Niekerk & Von Solms, 2005). Without adequate security knowledge, users would not behave securely, and subsequently they might apply a security control incorrectly.

The aim of this research study is concerned with investigation the security knowledge required to influence the employee behaviour in order to guide the organisations to instil the security knowledge required between the employees to influence their behaviour when interacting with information assets to minimize the risk.

1.2 Problem Statement

Many studies have revealed that organisation’s insiders pose risks to the security of information assets. The insider (e.g., employees) inside organisations could be responsible for most of the data breaches that occur, whether intentionally or unintentionally

(Symantec, 2017; Internet Security Threat Report, 2018; Verizon, 2014; Van Niekerk & Von Solms, 2005; Sohrabi Safa, Von Solms, & Furnell, 2016; Van Niekerk & Von Solms, 2010). The users of a system can be its biggest enemy (Vroom & Von Solms, 2004) and can cause serious risks despite the amount of money spent on the technical measures and on security related products (Von Solms, 2006). Focusing only on the technical aspects of security without considering how employees interact with the system is evidently inadequate (Parsons et al., 2015). The effectiveness of these technologies lies in the behaviours of the employees who access, use, administer, and maintain information resources (Da Veiga & Eloff, 2010; Van Niekerk & Von Solms, 2010).

Lack of knowledge in information security may jeopardize the organisation such as the increase of internal security incidents and give a negative impact to organisational effectiveness. Employees' error, mistake, ignorance, and not technology, is behind most of internal security incidents (Kitchenham & Charters, 2007). Furthermore, employees' attitudes and lack of knowledge of security issues are amongst the most significant contributors to security incidents (Von Solms & Furnell, 2016). The employee misbehaviour and harmful interaction with the organisation's information assets lead to internal security incidents. This, in turn, would cause negative consequences on the stability of the organisation and to maintain the availability, integrity and confidentiality of that information (Hogail, 2015). It is important for employees to be knowledgeable and behave in a way that will have a positive influence in protecting information. In order to achieve the desired behaviour from the employees in the organisation, it is necessary for the employees to have an adequate level of security knowledge regarding their supposed roles and responsibilities in the security process (Hogail, 2015). To achieve this, the employees need knowledge in information security which would ensure the effectiveness of information security in organisation which in turn can help to minimize the internal security incidents.

Based on the literature review, researchers have found a correlation between knowledge and behaviour in information security (Zakaria, 2004; Van Niekerk & Von Solms, 2010; Al-Hogail, 2015; Da Veiga & Martins 2015). However, the correlation between knowledge and behaviour was mentioned in prior studies without any given further details about the types of knowledge in information security and the impact of the knowledge on behaviour. Given that there are many different types of knowledge with respect to information security, it is not yet known which of them can influence an employee's security behaviour and in what way the behaviour is influenced by the knowledge. It is expected that each type of security knowledge will have different influence on an employee's security behaviour and therefore a model is needed to represent this relationship. Finally, the actual impact of security knowledge on security behaviour needs be investigated. By inculcating the employees with the required set of security knowledge, it is expected that the number of internal security incidents can be reduced.

1.3 Research Questions

The core research problems are translated into a number of research questions in order to answer them:

1. What is the security knowledge constructs required to influence employee behaviour?
2. How can the relationship between security knowledge constructs and employee behaviour be presented?
3. What is the impact of each security knowledge constructs to employee behaviour?

1.4 Research Objectives

The research questions have been translated into a number of objectives that are summarized as follows:

1. To identify the security knowledge constructs required to influence employee's behaviour.

2. To propose a model for the relationship between security knowledge constructs and employee behaviour.

3. To determine the impact of each security knowledge constructs on employee behaviour.

1.5 Research Scope

This study was conducted in the healthcare services sector. The healthcare sector is chosen because according to the studies presented by Ponemon Institute (2017) & Symantec Internet Security Threat Report April (2018), it was found out that the healthcare industry has the largest percentage of disclosed data breaches as shown in Figure 1.1. Moreover, 94% of hospitals in the US have suffered from data breaches which have caused the loss of millions of dollars. Therefore, conducting the study in the healthcare sector can provide a high impact in improving the sector.

This study is conducted on healthcare services in Palestine. An approval has been obtained from Palestinian Healthcare Ministry in order to conduct a survey. The total number of governmental healthcare services is five they are distributed in all the Palestinian cities. The scope of the study was narrowed down to healthcare services that use health information systems (HIS), and employees who use computer or laptop to perform their work in healthcare services. Their computers may contain a lot of sensitive information related to the patients, doctors, employees, and other healthcare organisations.

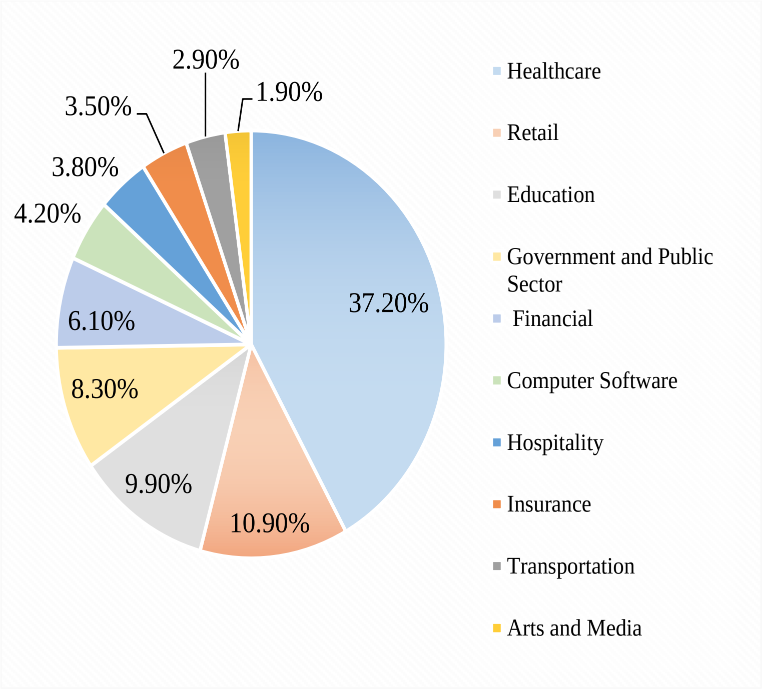


Figure 1.1 Symantec: Internet Security Threat Report (April 2018)

1.6 Organisation of Thesis

The organisation of the study follows the standard thesis format and the content of this document is organized into six chapters.

Chapter 1 provides the research background, problem statement, research questions, research objectives, research scope, and organisation of the thesis. Chapter 2 provides the literature review about the information security culture, security knowledge required to influence employee behaviour, security behaviour, organisational behaviour and the relation between behaviour and information security culture. Chapter 3 provides the research methodology used to answer the research questions. Chapter 4 cover the qualitative interview analysis and findings. Chapter 5 provides a research model and hypothesis development. Chapter 6 provides the analysis of data collected and findings. Chapter 7 summarizes the conclusion and future work.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This study examines the security knowledge required to enhance the security behaviour in the context of information security culture. In particular, the chapter provides a discussion of the general concepts and terminologies of information security culture. The discussion is organized as follows; section 2.2 presents information security concept. In section 2.3 presents the definitions of information security culture, literature review regarding information security culture and presents the relation between information security culture and organisational culture and behaviour. The role of human factor in the concept of information security culture as well as in insider threats, common risks posed by the insider also presented. In Section 2.4, the section provides an introduction to the definition of security knowledge and the studies in literature dedicated to security knowledge. Why focus on security knowledge to behaviour is also presented. A discussion on the constructs of security knowledge that contributes to the enhancement of employee behaviour also presented. Section 2.5 that contains security behaviour, specifically insider security behaviour. In section 2.6 behaviour theories and models were discussed that focus on knowledge and behaviour. In section 2.7, present a discussion on KAB model including, introduction to KAB model, review on studies that use KAB model to enhance and develop KAB model in information security, address the relationship between knowledge, attitude and behaviour. Furthermore, adapting KAB model and propose the variables in element of KAB model also discussed in this section. Section 2.8 discuss the interaction model between knowledge, attitude and behaviour in KAB model in order to reduce internal security incidents. Last, in section 2.9 provides a summary of the chapter and its contents.

2.2 Information Security

Information Technology is becoming a core element of almost all aspects of life such as business, industries, organisations and other sectors. This transformation leads to most organisations adopting the technology to perform daily tasks. Consequently, these transformations have introduced a lot of risks organisational information assets. The most important thing in information security is protecting information assets from being disclosed, integrity violation and denial of service. Therefore, information security is defined as the activity to protect information from a wide range of threats in order to ensure business continuity, minimize business damage, and maximize return on investments and business opportunities (Parsons et al., 2015). Other researcher define information security as the business requirement to protect the organisation’s investment in its information assets (Pipkin, 2000). The Information Security Management System defines information security as a preservation of confidentiality, integrity, and availability of information, in addition with other properties such as authenticity, accountability, non-repudiation and reliability (Whiteman & Matort, 2014).

Information security is not a purely a ‘technical’ issue, it is also non-technical issue associated with ‘people’. The technical approach fixates on deploying technology like cryptography, authentication methods, firewalls, and security controls models to mitigate threats. The technical approach applies technical controls to computer hardware, software, or firmware (AlHogail & Mirza 2014). With all the development technology, it has been noticed that the number of breaches due to the human factor have risen. Security controls often require some form of human involvement and the humans’ role is very important in the information security process (Van Niekerk & Von Solms, 2010). In most organisations, managing information security threats focuses on managing technology and process, but little efforts are made to manage people (Van Niekerk & Von Solms, 2010; Parsons et al., 2015; Von Solms & Furnell, 2016). Organisations will not be able to protect the integrity, confidentiality, and availability of information assets if they ignore the human factors.

Information is considered to be very essential for organisations to the extent that it is regarded as a key asset of a given organisation (Van Niekerk & Von Solms, 2010). Therefore, protecting this information is crucial to ensure the stability of the organisation and to maintain the availability, integrity and confidentiality of that information. A recent study by Ponemon Institute (2018) indicates that many organisations have lost billions of dollars as a result of information breaches or information violations. These breaches have also had some negative effects on customer trust. Among the major threats faced by an organisation are the employees' acts and behaviours especially when they interact with the organisation's assets.

In information security, employee error, employee mistakes and employee negligence contribute to most of the data breaches in organisations (Da Veiga & Eloff, 2010; Martins & Eloff, 2002; Schlienger & Teufel, 2003). Hence, concentrating only on technical measures to protect an organisation's assets without any consideration of the employees is clearly inadequate (Appari & Johnson, 2010; Samy, Ahmad & Ismail, 2009). Thus, on one hand, employees play a prominent role in creating threats to an organisation and on the other hand, they can play a key role in protecting against, or preventing, such breaches. Therefore, organisations should focus on employees' behaviour, attitudes, knowledge, assumptions and awareness in order to guide the employee behaviour when interacting with organisation assets. The effectiveness of any type of security system depends on employee's behaviour towards the organisation's information assets (Boujettif & Wang, 2010).

Employee need knowledge in information security to ensure the effectiveness of information security in the organisation which in turn can help minimize the internal security incidents. It will help employees to be more aware of the security risks and of their responsibilities toward information security, and it should enable them to act in a secure manner to reduce the risks of their misbehaviour and harmful interaction with the information. The following section discuss the information security culture to promote an appropriate security behaviour between the employees with in organisation.

2.3 Information Security Culture

This section aims at formulating the understanding of the concept of the information security culture and presents a summary of pervious works that aimed at establishing and managing that culture. Firstly, it explores the literature in order to provide a definition of the information security culture which serves as a reference of understanding. Next it presents and reviews the key literature to identify the related works that discuss various issues of information security culture.

2.3.1 Information Security Culture Definitions

Information security culture is a sub-category of the organisational culture as information security has become an organisational function. It causes the preservation of information security to become a natural practice in the daily activities of every employee such that the organisation assets are always protected (Schlienger & Teufel, 2003).

Past literature (Schlienger & Teufel (2003), Thomson, Solms & Louw (2006); Von Solms (2006);Vroom & Von Solms (2004)) claimed that information security culture has to be viewed as a goal to be accomplished in order to develop a culture that covers the entire activities and guidelines required for information security to be part of the daily activities of every organisational employee. Some other studies like (Martins & Eloff (2002); Ngo et al. (2005) see information security culture as how things are done by employees and the organisation as a whole to be naturally consistent with information security principles. Some of the more popular definitions of the concept of information security culture in literature are provided below;

- Dhillon (2007:2):"*The collection of human attributes such as behaviours, attitudes, and values that facilitate the protection of all the information in the organisation".*
- Da Veiga & Eloff (2010: 198):"*The attitudes, assumptions, beliefs, values and knowledge that employees use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour evident in the artefacts and creations that become part of the way things are done in the organisation to protect its information assets".*
- Ngo et al. (2005:68): *"Information security culture as a goal to be achieved by the creation of a culture that should support all activities in a way that information security becomes a natural aspect in the daily activities of every employee job".*
- Sabbagh et al. (2012:33) :*"The way our minds are programmed that will create different patterns of thinking, feelings and actions for providing the security process".*
- Alhogail & Mirza (2014:3):*"The collection of perceptions, attitudes, values, assumptions and knowledge that guide how things are done in the organisation in*

order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees' security behaviour *in a way that preserving the information security becomes a second nature".*

- Alhogail (2015:567):*"Information security culture guides how things are done in organisation in regard to information security, with the aim of protecting the information assets and influencing employees' security* behaviour*".*

- Martins & Eloff (2002:205): *"The perceptions, attitudes and assumptions that are accepted, adopted and encouraged by the employees in the organisations in relation to the information system".*

- Malcolmson (2009:361): "*Security culture is candidate by the assumptions, values, attitudes and beliefs held by the employees of an organisation and their behaviour could potentially impact the security of that organisation and that may or not may have an explicit known link to that impact".*

- Da Veiga & Eloff (2010:198): "*An information security culture is defined as the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artefacts and creations that become part of the way things are done in an organisation to protect its information assets. This information security culture changes over time".*
- Zakaria (2007:38)*:* "*An information security culture is a learned process. The existence of a suitable information security culture can guide everyone in an organisation to learn about various aspects of information security which can then be adopted into his or her daily work routines*".

It is clear from above that there are various definitions of information security culture. In general, the definitions given in the literature can be divided into two groups. The first group defines information security culture as guides that can influence security behaviour (Alhogail & Mirza, 2014, 2015; Ngo et al. 2005). The second group defines information security culture as the result of security behaviour (Da Veiga & Eloff, 2010; Malcolmson

2009) . For this thesis, the definition of the second group is adopted that the behaviour will lead to culture after it has been practiced for a long time. The aim of this research study is concerned with investigation the security knowledge required to influence the employee behaviour in order to guide the organisations to instil the security knowledge required between the employees to influence their behaviour when interacting with information assets to minimize the risk. Based on the definition given in the literature, the culture will happen after the behaviour is practiced for a long time. This can then help to develop an information security culture amongst employees in the organisation.

The employees in organisation deals with information assets while performing his/her daily work routines in organisations'. Employees (i.e. insiders) need to perform security tasks to ensure the security of the information assets and when the employee done such security practices these security tasks as a part of his job, these tasks can become a part of their daily routine, and when this work becomes most common between the employees in the organisation then their behaviour will be guided towards securing the organisation information assets. As time passes, this will lead to create an information security culture between the organisation employees. Therefore, it is clear that we can develop an information security culture within an organisation because it is also a learned process. The presence of an appropriate information security culture can be used as a guide to direct the employees in their learning of different information security practices, which they can later be adapted in their day-to-day work routines. Thus it determines the corporation activities. In order to go in-depth, the related work that have been done in information security is explained in following section.

2.3.2 The Information Security Culture and Organisational Culture

In the field of organisational studies, the primary reason behind the increasing interest in culture is the sub-cultural dynamics in the organisation that can lead to a better understanding of how new technologies influence or are influenced by organisations' (Schein, 1992). In addition, culture is a crucial component influencing the management effectiveness across nationalities, ethnicities and religious boundaries (Schein, 1992). Culture can influence the organisational learning, development and planned changes (Schein, 1992) and can be an asset if it facilitates acceptable practices in the workplace and a liability if it promotes adverse practices (Longhurst et al., 2017). Culture in an organisation can be viewed to be good if it relates to acceptable workplace practices or bad if it is confined to unacceptable workplace practices (Longhurst et al., 2017). Besides, a good culture can also be referred to as a strong or appropriate culture that can influence the way people perform their work routines within an organisation (Baldwin et al., 1999). After the cultural aspects in an organisation have been analysed, it is possible to determine whether an appropriate culture has been cultivated.

According to Schein (1992), the concept of culture is not only appropriate to organisational level analysis but also to assist in understanding what is going on within an organisation, with occupational groups and subcultures have to cooperate and work together. In case a problem arises, it may be considered as failure to communication, or a breach in teamwork, or any other related issue. When the culture is understood, then the problem may probably be related to intercultural communication (Schein, 1992).

Moreover, culture establishes a sense of identity to the members of the organisation and help to increase their commitment to the organisations (Smircich, 1983). For instance, upon internalizing the values of the organisation, employee will realize their work is intrinsically rewarding and they will be motivated to identify with their colleagues at work (Nelson & Quick, 1996). This can increase employees' motivation, which in turn can encourage employees to become more committed to their jobs.

According to Lundy (1993), the most popular and simplest definition to organisational culture is “the way things are done here”, and based on Robbins (2001) study, organisational culture can be viewed as the organisational personality. Meanwhile, (Da Veiga & Eloff (2010) described culture as the social glue that binds the organisational members together.

Furthermore, organisational culture also functions to shape the employees’ behaviour. Nelson & Quick (1996) state that cultural elements such as `norms' can guide behaviour as these norms are expected modes of behaviour that are accepted as the organisation’s ways of doing things (Huczynski & Buchanan, 2001). For instance, in some companies a ‘clean desk’ policy is implemented, where the workplace desks should be cleared of paperwork at the end of the day.

We can say based on the above, finding a suitable security culture in organisation can help the employees in organisations to adhere and perform the security tasks and practices. It is a must to integrate security tasks to day-to-day routines in order to develop a security awareness culture among employees. In other words, every employees should be aware of how and what to examine, secure, determine, respond and reflect suitably when dealing with information assets.

Information security culture is one of the top significant issues in organisational culture and it is referred to as a sub-category of organisational culture that covers daily processes, activities, guidelines and practices among the employees, assisting them in safeguarding information assets in the organisation and mitigating the risks posed on them (Zakaria, 2006). According to Dojkovski et al. (2007), the local culture of the organisation has a significant impact on the formulation of the information security culture.

A number of studies in the literature have discussed the relationship between organisational culture and the information security culture. For instance, Ashenden (2008) studied the challenges facing information security culture from an organisational perspective. Chang & Lin (2007) presented a model of the relationship between organisational culture and ISM that quantifies the impacts of organisational culture traits on the effectiveness of information security culture. Lim et al. (2009) have presented a framework to assist organisations in determining the extent to which the desired information security culture is embedded into organisational culture. Moreover, Ruighaver et al. (2007) have discussed the effect dimensions of organisational culture on information security culture. Connolly & Lang (2013) studied the role of information security culture in organisational settings to achieve information systems security. Findings from these studies indicate that organisational culture has a major impact on both information security management and information security performance.

In organisations, all individuals are expected to participate in the information security process of that organisation. Those individuals have different assumptions, attitudes and values towards the information system implementation and security. Rapid technical advances bring also an increase in the range of tools used for conducting unauthorized behaviours. Therefore, it is important to understand the underlying principle values, beliefs and assumptions that drive users' behaviour. This is further complicated by the rapid rate of changes in the information systems environment with respect to security threats, which makes it unwise to assume that individual knowledge and skills will be current and remain as expected (Alnatheer & Nelson, 2009; Da Veiga & Martins, 2015).

In Hogail (2015) argued the information security culture is assumed to be part of the organisational culture as information security has become an organisational function. It supports all activities in a way, that preserving information security becomes a natural aspect in the daily activities of every employee (Schlienger & Teufel, 2003). The local organisational culture will highly affect the formulation of the information security culture (Dojkovski et al., 2007). To achieve a secure environment for information assets, information security practices should become part of the corporate culture of an organisation. This corporate culture guides the activities of the organisation and its employees by placing constraints upon the activities and behaviour of employees and by prescribing what the organisation and its employees must, can, or cannot do (K.-L. Thomson et al., 2006) and influences employees' behaviour. Therefore, it should be used to establish the security behaviour of employees (Lopes & Oliveira, 2014).

Organisational behaviour is an interdisciplinary field dedicated to the better understanding and management of people at work. They also define three basic levels of behaviour in an organisation, namely the individual, group and organisational level (Robbins, 2001). Employees will behave according to what is perceived as correct and acceptable and specific organisational behaviour will surface on each level. Such behaviour also encompasses employee attitudes and the way in which they influence actual performance in organisations (Hellriegel, Slocum & Woodman, 1998).

A number of studies in the literature have focused on organisational behaviour for example, Martins & Eloff (2002) designed an information security culture framework based on the concepts of organisational behaviour (Robbins, 2001) and what constitutes information security. They identified information security controls that can also be referred to as principles on the individual, group and organisational level of organisational behaviour tiers and that could influence information security culture (Martins & Eloff, 2002), for instance policy, awareness and change. This theoretical perspective provides the foundation for the information security culture assessment instrument and the items developed by the researchers to assess an information security culture. Findings from these studies indicate that organisational culture has a major impact on providing information security to protect the organisation's assets.

Moreover, Martins & Eloff (2002) focused on organisational or employee behaviour on an organisational, group and individual level aimed at cultivating an information security culture. Furthermore, Martins & Eloff (2002) use the definitions of organisation culture and organisational behaviour to define information security culture. They see it as a set of information security characteristics valued by the organisation, such as integrity, confidentiality and availability of information. They also relate it to the assumption about what behaviour is regarded as acceptable in protecting information and what not. The concept of an information security culture further extends to the type of behaviour that is encouraged to protect information and that which is not. The researchers’ emphasis is on the behaviour that is present as a result of the attitudes and values of employees, since such behaviour leads to the development of an information security culture of the organisation. The organisational behaviour focuses on employee behaviour and how this could relate to vulnerabilities in the computer and information systems (Robbins, 2001; Vroom & Von Solms, 2004). It is this behaviour that in time establishes the information security culture that forms part of the overall organisational culture.

2.3.3 Human Factor in Information Security Culture

Businesses are largely dependent on information system, mobile computing, the Internet, clouding, and other methods to accomplish sustainability and productivity. However, this invites a new type of threat that has to be dealt with to safeguard the information assets of the organisation. Whenever unauthorized individuals can access information, information becomes vulnerable, and in turn, the misuse, loss or damage to information can negatively impact the overall organisational performance. Hence, several issues arise when it comes to protecting information assets.

Generally speaking, the use of technical method to safeguard organisational information assets is no longer sufficient as information security is no longer a technical issue but a human one. The control of security needs human role combined with technical role in information security process (Van Niekerk & Von Solms, 2010).

The system users could be its top enemy and they can cause serious risk regardless of the huge investment incurred on security products and technical measurements (Von Solms , 2006;2004). In this regard, majority of organisations have been trying to manage information security threat by concentrating on both technology and process. Accordingly, they incur costs on technical measurement and products that have the potential to improve the organisations' security (Niekerk & Von Solms 2006; AlHogail & Mirza 2014). In contrast, organisations pay little attention to the way employee behaviour is managed and the provision of information security culture and security knowledge to employees. To this end, it is crucial to pay attention to the human factor through the management of perceptions of employees along with their attitudes and knowledge. Activities conducted to safeguard the organisation from threats that ignores human factors and their behaviour would leave the organisation's assets availability, integrity and confidentiality at risk. Hence, protection of information systems from human threats like human ignorance, careless and misuse of assets should be deemed as the top concern for information security experts (Da Veiga & Eloff, 2010).

The major reasons that bring about the ignorance of insider threat and human factor within organisations were highlighted by Colwill (2016) as follows: (1) the organisation's lack of awareness of the risks coming from employees; (2) the organisation's fear for its reputation and thus, is in denial of any internal threat from employees; (3) majority of organisations who are aware of the threat from employees are clueless as to how to deal with it or how to resolve it. This is evidenced by the fact that several organisations keep insider errors or attacks private and this makes the estimated scale of the problem to be inaccurate. On the basis of the report provided by the PWC (2013), majority of organisations (70%) do not report their worst security incident.

There are a number of researchers who discussed the challenges of human factor in formation security. For example, a number of researchers have suggested that successful information security management needs to achieve a better understanding of the social aspects of the organisation, in particular the human element (Thomson et al. 2006;

Ashenden 2008; Veiga & Eloff 2010). Humans are usually difficult to manage in the context of information security. In fact, humans are not very predictable because they do not operate as machines where given the same situation, machines will operate in the same way.

2.3.3.1 The Human Factor and the "Insider Threat"

The human factor is deemed to be an "insider threat". Insider threat refers to "intentionally disruptive, unethical, or illegal behaviour performed by individuals who possess internal access to the organisation's information assets" (Stanton, Stam, Mastrangelo, & Jolton, 2005) . According to Jouini, Rabai & Aissa (2014), "Internal threats related to the organisation employees occur as the result of employee action or failure of an organisation process". Insider threats also cover unintentional disruption from individuals who can access the information assets of the organisation (K.-L. Thomson et al., 2006). The human that should be considered are all the individuals in the organisation who have access to information, from top-level managers to clerical staff.

Several studies including Hu et al. (2012); Nelson & Simek (2006) reported a significant emerging threat to information security and such threat is from employees themselves. This is aligned with the Colwill (2009) study that revealed insider activities to account for 70% of fraudulent activities but despite this fact, 90% of security controls are directed towards external threats. The human as 'insider threat' premise is one of the top IT security challenges that organisations are facing and among the most challenging to safeguard against as evidenced by (Hu et al., 2012; Stanton et al., 2005). These incidents based on severity could cost organisations from a few lost employee's hours to negative publicity or even financial damage. Moreover, since WikiLeaks published classified information through insiders, many organisations and security experts paid more attention to the dangers insiders can pose to organisations. A security breach survey by PWC (Price Waterhouse Coopers) in 2015 showed that 28% of large organisations reported security breaches are caused by staff. 57% of small organisations suffered insiders related security breaches and 36% of the worst security breaches were caused by unintentional human error.

To compound the matter further, the development of mobile devices enabled employees to have sensitive and confidential information in their personal laptops, USB storage and smart phone and when this is lost, it could put the information assets at risk. Despite these clear implications, many organisations lack plans and strategies to steer clear of employee threats as reported by the PWC (2013). The report indicated that 42% of the organisations lack security awareness and training for employees and as such, this calls for the adoption of security solutions that takes into consideration of the human factor within organisations.

2.3.3.2 Common Risks Insiders Pose to Information Security

There are many examples of employees’ behaviour that could pose a risk to the security of the organisation’s information. In this section, a number of threats caused by insiders are presented.

Among the popular threats to the information security in an organisation is the erroneous behaviour of employees (K.-L. Thomson et al., 2006). One of the top trends in security threats that organisations are facing is negligence of employees as evidenced by the Ponemon Institute (2015) study. The study reported that 75% of security threats stem from negligence of employees. In other words, ignorant or careless employees may bring about unintentional information security risks through the following ways (Dojkovski et al., 2007):

- By retrieving spam mail.
- Opening an e-mail attachment hosted by a virus.
- Unaware of information security policy of the use of external devices.
- Negligence from employees could leave then network of the organisation vulnerable to malware, viruses, worms and Trojans and this may infect the whole system.
- Additionally, attaching their personal devices such as (USB drives, external hard disks) to the system without taking precautions can lead to the exposure of the organisation’s network to security threats.

Aside from the above, employees’ negligence could also lead to leaking of confidential information out of the organisation, as according to PWC (2013), 34% of cyber incidents were caused by unintentional exposure of private or sensitive data. Also in this regard, majority of employees bring their mobile devices wherever they go and these may contain sensitive work-related information that could expose data to risks when such devices are lost or stolen. In light of outside relationships, employees sometimes allow their families and friends to make use of organisation's computer or network and in this case, some sensitive data could be obtained by third parties and this could expose the assets of the organisation to security risks. Moreover, the lackadaisical disposal of personal records or the careless sending of documents to the wrong recipients could cause security threats (Renaud & Goucher, 2014).

Generally, employees possess limited knowledge on security. Based on a security survey on employees, majority of them (62%) have limited knowledge concerning information security (PWC, 2013). Another security survey indicated that although 98% of the surveyed respondents possessed anti-virus software, 52% of them were still virus-infected (Richardson, 2007).

Literature showed that employees failure to adhere to the information security guidelines and policies established can be the cause of majority of the breaches to information security (Parsons et al., 2015). Employees that own personal devices that get plugged into the company's network are posing risks to the information assets of the organisation. More importantly, personal devices could be utilized to copy considerable volumes of sensitive data, information or programs from the company network. Furthermore, given that some of the employees commonly download non-work related contents, they could be putting the IT system at risk through infected contents.

In addition, there is a possibility that some employees may maliciously crack the organisation IT system to steal information, misuse, or deliberately challenge the business from within (McAfee 2015). In fact, leaked confidential information by insiders to competitors or to the public, can lead to disturbing financial consequences. To stress that, in order for a hacker from outside the organisation to gain access to data, he needs to figure out how to break into the network first, and then locate the target data without being detected by security systems, whereas employees within the organisation have direct access to the data. Based on insider survey conducted in 2015, 31% of US cybercrime done by insiders involve theft of information such as customer and financial records (Pwc, 2013). Very often costly security incidents happen when organisation's insiders leak confidential information to other parties outside the organisation (Nelson & Simek, 2002).

Moreover, some of the activities that can render organisational data susceptible to security threats include:

- Browsing unsafe websites.
- Downloading suspicious software.
- Sharing passwords among employees.
- Disregard for organisation policies. This can be exemplified by some users, who have the habit of writing their passwords on the desk in the office, or on the monitor.
- Some who leave their computer on after work without safeguarding them or following security protocols when it comes to computers and laptops.
- Others may inadvertently disclose their personal information or that of the organisation to the public through social media.
- While some others are prone to accessing unsafe websites and go through scam emails or fraudulent websites through which the attack can be initiated.
- Unsuspecting users have no qualms of entering their user names and passwords, their bank accounts, email accounts or even the organisation’s account in bogus websites (phishing).

According to the statistics reported by Google, in 2013, 10,000 websites are daily blacklisted, with vast majority of malware attacks stemming from legitimate sites.

It is evident from the above that computer users are the weakest link in the chain of computer security and this is evident in activities such as (1) accessing fake or unsafe websites, (2) installing malicious programs in the laptops or company computers that will unintentionally disclose data to unauthorized third parties. Employees will then fall victim to the attack by exposing organisational assets to risk. Their carelessness, negligence and insecure culture knowledge are what driven them to do so.

As a response to insider posed risks, many organisations have implemented a range of administrative and technical measures within an overall information security management system that is based on standards, policies, procedures and best practices (Dojkovski et al., 2007).

2.3.4 Related Works on Information Security Culture

The related studies concerning information security culture was gathered using systematic review and analysed using qualitative content analysis. Such analysis uses a subjective interpretation of the text content using a systematic process of classification that codes and identifies themes or patterns within the text.

A thorough review of literature highlighted papers dedicated to information security culture frameworks that discuss various issues of information security culture, researchers have proposed different frameworks to guide the research and application of the information of security culture. Further most of the frameworks proposed based on various assumptions and issues.

An investigations and reviews the key literature on studies that are dedicated to security knowledge as a significant factor in information security culture and any other literature that discuss the relation between knowledge and behaviour in information security culture. The review on information security culture frameworks is summarized in the following paragraphs:

To begin with, a framework proposed by Chia et al.(2002) whose organisational culture framework was based on Detert et al. (2000). Their framework concentrated on heightening information security awareness among employees to determine the effect of organisational culture on information security culture. They reached to the conclusion that administration support and employee awareness are both top factors of information security culture.

Moreover, Schlienger & Teufel's (2003) framework was based on internal marketing and it aimed to conduct an analysis of information security culture in organisations to develop and improve their culture. They based their framework on Schein’s model that involved several steps; the first being pre-evaluation followed by strategic plan, operative plan, implementation and post-evaluation. The steps are susceptible to change, evaluation and maintenance. This study was not practically tested to examine whether or not it can change or maintain the security culture of the organisation.

Also, an integrated Bloom learning taxonomy model was proposed by Van Niekerk & Solms (2005, 2006); Van Niekerk & Von Solms (2010) to examine information security culture. They based their frameworks on Schein's model and they contended that for the provision of an effective information culture in organisations, it is a must to furnish security knowledge to employees and this can be viewed as the fourth layer of Schein's model (the knowledge layer). Their study aimed to set up an effective information security culture in organisations and accordingly. They highlighted that the Schein model describes the organisational culture instead of information security culture.

In addition, Koh et al. (2005) proposed a framework that was built on Schein's model that was connected to organisational culture theory, intending to examine the way security governance influences security culture in light of responsibility and ownership and security. The findings showed that the structural and functional mechanisms in security governance took top positions as influential factors.

In the same line of study, Zakaria (2006) brought forward a framework that had its basis on Schein's (1992) organisational culture model to develop data collection methods for research studies dedicated to information security culture throughout organisations. The use of the following methods of data collection was recommended by the author; questionnaire, semi-structured interviews, direct observation and documentation review methods.

Ruighaver et al. (2007) brought forward a framework that they developed on the basis of the organisational culture dimensions framework proposed by a prior work by Detert, Schroeder & Mauriel (2000) . The dimensions include truth, time, motivation, stability, control and orientation – all these dimensions enhance the understanding of the security culture of the organisation and the steps needed to obtain a particular organisational culture. Each of the above mentioned dimensions was examined in light of its use to construct information security culture. According to the authors, the ideal security culture, is the one that balance between both internal and external factors.

Moreover, a framework was also developed by Dojkovski et al. (2007) to improve the information security culture implementation in SMEs, Australia. They provided a detailed discussion of the challenges faced in the development of security culture within such enterprises. The researchers also highlighted other factors influencing information security culture including national and ethical culture, governmental initiatives to raise awareness and information security benchmarks, as well as vendors illustrating trustworthiness to SMEs. The authors also highlighted internal factors that significantly influence information security culture and they included both governance and organisational culture. They further elaborated management factors of security policy and budget and earning factors of workers, including e-learning, training, awareness and education to develop and facilitate an environment for information security culture implementation within businesses. Lastly, the authors urged top managers to concentrate on promoting employees' awareness of information security culture and to draw up strategic plans to guarantee that such culture is permeated throughout the organisation.

Also, Chang & Lin (2007) sought to examine the organisational culture-information security management relationship to determine the effects of organisational culture traits on the effective ISM implementation. According to the authors, majority of organisational features have to be assisted by cooperation, innovation, consistency and effectiveness.

Added to the above frameworks in literature, Alnatheer & Nelson (2009) also proposed a framework to shed light on information security culture and best practices in the Saudi Arabian case. The framework involved steps to achieve information security management and details of the cultural factors facilitating the setting up of information security culture in the firm. The framework's main objective is to guarantee that security culture is integrated in the day-to-day practices of Saudi organisations. The authors provided the major factors influencing information security culture which are organisation's governance, regulatory and legal environment and other corporate aspects. They reached a conclusion that national culture influences organisational culture and security culture.

Similarly, Lim et al. (2009) framework was aimed to assisting organisations to determine if the needed information security culture is integrated in the culture of the organisation. They examined the relationship between both cultures with the framework based on eight-dimensions of organisational culture adopted from Detert et al. (2000). The authors contended that integrated the concept of information security culture throughout the organisation can affect the security behaviour and actions among employees.

Meanwhile, Da Veiga & Eloff (2009) proposed a comprehensive framework for the evaluation and enhancement of information security culture practice of organisations. They initially identified information security elements that should be adopted by the organisation which are process, human and technical threats. These could disrupt the setting up of an effective information security culture. These elements were further categorized to encapsulate every individual, group and organisation relationship of information security behaviour. The framework provides a description of the integration of information security culture in the organisation. Nevertheless, the author's framework failed to demonstrate internal relationships and the expected influences of various information security elements.

Another similar framework came from Alfawaz et al. (2010) study that identified the specifications of organisational culture according to information security practices through the determination of knowledge, skills and activities of employees that may affect and improve individual and group practices in light of information security culture management. The model focused on the effect of national culture on organisational culture and the authors provided four types of behaviour namely, knowing-not doing, not knowing-doing, not doing mode, and knowing-doing mode. The authors contended that the employees' behaviour could be modified from one model to the next according to their role, the organisation's technology and the security situation and awareness.

In Hassan and Ismail's (2012) study, they proposed a conceptual model in the context of the healthcare environment. On the basis of their literature review, they determined several factors influencing information security culture including information security awareness, behaviour, change management, knowledge, and organisational system and security requirements. Their framework however seemed to fail in identifying the relationships among factors and their effects on information security culture.

In a similar line of study, Shahri et al. (2013) presented an extensive framework to create effective security for health information systems that is built on security culture and security awareness. Their framework is aimed at enhancing human behaviour through security awareness and security culture provision in the context of e-health information system. According to them, security awareness and security culture are the top aspects that have to be considered to set up an effective health information security framework. Their proposed framework however lacks depth in terms of the identification of the components and factors and the connections among them.

A framework contribution also came from Metalidou et al. (2014), focusing on the factors that impact end-user behaviour, which are lack of awareness, lack of motivation, belief, behaviour and insufficient technology. Added to this, the authors showed that the top issue that an organisation should address is the promotion of security awareness among employees via education and training. Moreover, it was found that the weakest link in security area was the human factor which made them to suggest some factors that can influence human acts in organisations.

Aside from the above frameworks, Hayaati et al. (2015) proposed a conceptual model for ISM e-learning that concentrates on the cultural views of people. The model provided a description of the connections between the dimensions linked to ISM e-learning stakeholders. The model also addressed the behaviours among stakeholders and their actual views. The study illustrated the dimensions of the conceptual model to include threats, stakeholders, cultural view and ISM components.

In Chen et al. (2015), the authors proposed a model to examine the effect of information security awareness initiatives on the engenderment of security culture. They found that security education, training and awareness (SETA) programs and security monitoring significantly and positively affected security culture and the awareness of employees of the organisational security policy. They also found awareness of security monitoring to be positively related to security culture. Their framework was geared towards assisting the establishment of information security culture in organisations.

Meanwhile, a framework that concentrates on security behaviour was presented by Hogail (2015) based on assumptions, attitudes and human factor diamond (management, responsibility, preparedness, society and regulations). In other words, their framework integrates human, organisation, strategy and technology factors together to assist the implementation and adoption of information security culture within organisations. It demonstrates issues linked to human behaviour that would bring about the establishment of a secure environment for the organisation’s information assets. The issues were discussed systematically through the use of STOPE model (strategy, technology, organisation, people and environment) to guarantee its comprehensiveness. The issues were then transformed into distinct activities and tasks that related to the human factor diamond. The change management principles were provided along with the cultivation process that directs the information security culture functioning in organisations.

Finally, Da Veiga & Da Veiga (2016) reported statistical findings that information security culture of employees, who were privy to the information security policy, was positive and significant in comparison to their non-privy counterparts. Stated clearly, the reading of information policy contributes to a positive influence on information security culture. The authors stressed on the value of awareness initiatives concerning information security policy that motivates the prioritization of sufficient policy and its relay to the employees.

It is evident from the above studies that majority of the frameworks proposed in the literature were geared towards addressing issues and factors that are related to information security culture. Added to this, the proposed frameworks developed according to the assumptions and environments. For example, some of the frameworks concentrate on human factors (i.e., provision of awareness, training and education programs), while some others focus on factors affecting information security culture.

The above review also aims to focus on the studies that are dedicated to the security knowledge as a significant factor in the development of security culture. In the studies such as Zakaria (2004); Van Niekerk & Von Solms (2010); Al-Hogail (2015), where the authors argued that knowledge and behaviour have to be integrated as significant factors in information security culture studies where knowledge directs the employees' behaviour in organisations.

More importantly, the employees in the organisation serve as the primary threat to the assets of the organisations (Da Veiga & Eloff, 2009; Martins & Eloff, 2002). According to Appari & Johnson (2010), human error leads to various data breaches in organisations and employees have a key role in the creation or prevention of threats towards the organisation. In this regard, the employees' security behaviour is directed by the required knowledge. In other words, knowledge is a significant factor in the management of perceptions, attitudes and actions guiding the interactions of employees with the assets of the organisation. To minimize the risks from the employees, their behaviour should be enhanced and promoted. Thus, focus should be placed on enhancing human security behaviour by focusing on the security knowledge required for the employees.

The above mentioned premise was supported by Van Niekerk and Von Solms (2010) who included another layer to Schein's model, which is a knowledge layer. The original of Schein's model comprised of three layers, it provides a description of organisational culture but not information security culture. In the fourth, added knowledge layer, the model is enhanced as it describes information security culture rather than organisational culture. A majority of the frameworks discussed earlier were created on the basis of the three-layer model proposed by Schein, indicating the lack of studies on information security culture that deemed knowledge as a significant factor as highlighted by Van Niekerk & Von Solms (2010).

Among the few studies in literature that addressed the relationship between knowledge and behaviour is Hogail (2015). The study found a positive relationship between knowledge levels and the behaviour of employees. Knowledge level significantly impacts information security behaviour and knowledge must be considered as an important element of the information security culture and related works.

In the same line of study, Rashid, Zakaria & Zulhemay (2013) contended the need for every employee to understand the significance of setting up of information security for the protection of the assets of the organisation. It is thus required to relay security knowledge to all employees. To this end, the knowledge-behaviour relationship was supported by Zakaria (2006); van der Spek & Spijkervet (1997), but the authors did not provide any detail on the types of knowledge that should be related to employees to improve their behaviour in relation to information security culture.

Evidently, employees need to have a suitable behaviour and attitude towards information security and this can be promoted through the provision of security knowledge to them. Also, their knowledge and behaviour have to be aligned for an effective information security. In relation to this, studies focused on security knowledge required to influence human behaviour are still scarce, and such studies should cover the impacts of security knowledge on employees’ behaviour in information security culture. This highlights the gap on security knowledge in literature.

In reference to the definitions of information security culture, employee behaviour is highlighted to be capable of accepting or rejecting to do a task in information security, illustrating the role of knowledge in guiding the employee behaviour in organisation, that a correlation exists between knowledge and employee behaviour calls for the focus on security knowledge required to influence the employee behaviour.

2.4 Security Knowledge

Present organisations are dependent on information systems to go through their functions and to ensure their survival and success. The most valuable asset of an organisation has become information and thus, it is crucial for organisations to protect their information. The protection process of information resources is referred to as information security and it is comprised of several processes, with most of them depending on human behaviour, human actions and human reactions. Stated clearly, human interactions with the information assets are managed through knowledge and hence, it becomes crucial to concentrate on the security knowledge of the employees in the organisation.

Employees within the organisation can pose as the top threat to the information security of the organisation through their intentional actions or negligence (Verizon, 2014). Therefore, the lack of employee knowledge of security techniques could lead to its misuse or misunderstanding and this may threaten the firm’s information assets. To this end, employees have to understand and know the security knowledge to decrease the risks to information assets and the risks from employees’ misbehaviour that could harm the information assets of the organisation (Martins & Eloff, 2002; Van Niekerk & Von Solms, 2010).

2.4.1 Security Knowledge Definition and Importance

In organisations, it has become necessary to provide security knowledge for the organisations employees to protect it from insider. Providing security knowledge to employees can help safeguard information assets, affect employee behaviour and decrease security incidents. Employees should possess sufficient security knowledge to safeguard the assets form security threats and vulnerability. Security knowledge and others security terminology has been defined in different ways by experts in the topic. Some of the more common definitions are given below.

- Sohrabi Safa et al. (2016:72): *” Knowledge refer to the theoretical or practical aims to understand the fact, subject, value, information or skill collected through experience or education”.*
- Kaur & Mustafa (2013:278): *“ Knowledge refers to the focus of what an employee knows; attitude focuses on what an employee think; and behaviour is about what an employee does”.*
- Kruger & Kearney (2008): the knowledge based on the users how to behave in specific events. For instance, knowledge is needed to scan the attachment files prior to downloading them and for minimized risk and viruses, only trusted sites can be accessed. Employees should also know how to manage passwords, including how to use strong passwords, changing them periodically based on organisational policy and keeping them confidential (Kruger & Kearney, 2008). Users who are equipped with proper knowledge has the ability to prevent threats and attacks, thus will help to increase the confidentiality, integrity and availability of information in the organisations (Sabeeh & Lashkari, 2011).
- Lilley et al. (2004:167) : *“knowledge is the entire set of insights, procedures and experiences that are considered true, and therefore guide the communications, behaviours and thoughts of people”.*
- Zakaria (2006:437): *“In information security context; basic security knowledge is about members in the organisation who are able to perform, learn and teach security tasks with respect to inspection, protection, detection, reaction, and reflection procedures on security matters”.*

The relationship between security and knowledge is encompassed by the term 'security knowledge’. Defining ‘security knowledge’ includes combining all related elements in security and knowledge. The element of security knowledge are extracted from the elements in security and knowledge, where knowledge elements are "information, value, experience, insight ", and security is defined as “The process of reducing risk or threats that can jeopardize an organisation.” In summary, security knowledge can be defined as:

The experience, values, and information provided by awareness and training education program that is practiced and shared between the employees in their daily work activities to reduce the risks and to protect the organisation’s information assets.

Applying security knowledge training can significantly impact the effectiveness of information security in organisation and at the same time reduce the security threats.

According to Zakaria (2006), knowledge has to be integrated to the processes of the organisation, its practices, activities, routines and norms, each employee has to be responsible for it in their day-to-day activities rather than just being left in documents and reports.

Despite the derivation of knowledge from information, it can also become information (Alavi & Leidner, 2001). They indicated that information is transformed into knowledge after processing in the mind of the individual, and after it is articulated and presented in text, words, graphics and other symbolic forms. This shows that knowledge can transform into information after it is shared in documents, books, policies, procedures, computers or other types of repositories. It reverts back to knowledge if it is relayed to other individuals (Hicks, Dattero & Galup, 2006).

In the organisation, knowledge is stored within documents, storage repositories, practices, routines, processes as well as norms, and in relation to this, there are two types of knowledge, which are tacit and explicit knowledge. Tacit knowledge refers to “the knowledge that stored in someone’s head”, which when non-internalized will be lost with the resignation and retirement of the individual who possess it (Nonaka & Takeuchi, 1995). On the other hand, explicit knowledge refers to “knowledge that is available to other individuals in whatever form such as codified knowledge” (Nonaka & Takeuchi, 1995) (Nonaka & Takeuchi, 1995). The codified knowledge can be formed as best practices, reports, policies, patents and procedures. Tacit knowledge has to be transformed to explicit knowledge for the knowledge creation and storage. When adapted to the information security, knowledge can be externalized to be learned by other employees and to share among them. This will in turn motivate employees to enhance their performance, improve learning and support teaching security practices and activities. Everyone's security practices combined together can help security experts to re-create effective security practices between the employees with on organisation.

In the same line of study, knowledge can be referred to as "the complete insight, experiences, and procedures that are true and that can be used as a guideline for communication and behaviour" (Van der Spek & Spijkevert 1997). Security knowledge management can be realized among employees through the individual management of knowledge (involving tacit knowledge), which can be later on transformed into a collective security practice (involving explicit knowledge), this premise was explained by Lilley et al (2004). In the information security of the organisation, each of the organisational employee have to be aware of how to perform security tasks, this can lead to create collective security responsibility among employees, and this shows that fundamental security tasks can be appropriated to the employees.

Further, the transformation of each individual process into one that involves collective practice, tacit knowledge has to be shared among the organisational employees Lilley et al. (2004). This can only be brought about by having brainstorming sessions, facilitating workshops, seminars, initiatives and discussions and boosting awareness programs in any and all (Nonaka & Takeuchi, 1995). Once the tacit knowledge becomes externalized during use, it transforms into explicit knowledge or what is referred to as conceptual knowledge as contended by (Lilley et al., 2004).

Based on the above, tacit security knowledge refers to knowledge stored in the individual's mind and is not usually institutionalized. Comparatively, explicit security knowledge refers to codified security knowledge that is collectively used as a security practice. In security knowledge constructs it is necessary to focus on collective security practices amongst employees rather than on the individual processes. This can, in turn, create a collective security responsibility. That means, everyone plays a part in taking security precautions. When all employees perform security tasks, it can help in influencing the employees' behaviour in organisation, and this, in turn, can help to reduce internal security.

It is impossible for organisations to ensure the integrity, confidentiality and availability of information assets without the consideration of employee behaviour in order to safeguard organisation assets. The provision of security knowledge to employees can work towards promoting successful implementation of information security culture in the organisation. Implementation of security knowledge will assist in instilling knowledge and in promoting understanding among employees of their roles and responsibilities in safeguarding information assets. This knowledge can be instilled through education, training, and awareness initiatives (Von Solms, 2006).

Employees' behaviour can be brought about by interlinking them with the information assets of the organisation and in this case, employees must have sufficient security knowledge level concerning their roles and responsibilities in the process of security systems. Also, security knowledge has to be developed in day-to-day activities supporting the business activities as part of the culture of the organisation. In other words, information security culture should become a natural practice in day-to-day employee activities. Cultivating each employee's security knowledge plays a crucial role in bringing about their desired behaviour. It is crucial that employees understand and act towards securing the information assets of the organisation (Rashid et al., 2013).

The required security knowledge will contribute towards the employees' understanding of their security roles and responsibilities and in adopting it in their daily activities (Williams, 2009). Information security culture is a culture that could modify the attitude of employees towards the adherence of security process, and such modification is expected to lead to behavioural changes (Safa & Von Solms, 2016). The provision of security knowledge in information security culture in organisations is expected to train employees to become security assets rather than risks (Ben-Asher & Gonzalez, 2015).

In the KAB model (knowledge, attitude and behaviour) sheds light on the knowledge role in behavioural change and the knowledge accumulation, with such knowledge accumulation leading to changes in attitude, and ultimately, changes in behaviour. Van Niekerk & Von Solms (2010) argued that if employees are capable of interpreting and understanding security policies and the related documents, they can behave in accordance with official security policies. They can also perform security activities in a way that their security behaviours are visibly displayed. Such visible security behaviours are significant as they can exemplify security practices that can boost organisational employees' motivation. After knowing the way to perform security activities in the daily tasks, the security practices can be included in the organisational processes, which in turn can help to develop a suitable information security culture within the organisation.

In relation to the above, Da Veiga, Martins & Eloff (2007); Van Niekerk & Von Solms, (2010) indicated that the setting up of information security culture in organisations is crucial for its protection. An information security culture has to be reinforced by sufficient security knowledge (Van Niekerk &Von Solms, 2005). Insufficient security knowledge would fail to bring about user's secure behaviour and they may end up incorrectly applying security control.

There are two dimensions to the human factor of information security and they are knowledge and behaviour. These two dimensions are interconnected (Van Niekerk & Von Solms, 2010). In fact, owing to the interdependence between the dimensions, it becomes impossible to ignore the effect of lack of security related knowledge on organisational sub-culture of information security. Hence, it is important that security knowledge be integrated into the day-to-day activities of every employee. Furthermore, Rashid et al. (2013) argued that human and knowledge are very interrelated because the organisation cannot create new knowledge without them. Therefore, knowledge originates and is applied in minds and only humans have minds that are needed in making decisions for competitive advantages.

2.4.2 Related Works on Security Knowledge and Behaviour

In this section, security knowledge studies in literature are presented and discussed. Among the studies, Van Niekerk & Von Solms (2010) provided a discussion of information security culture through a model that integrated Bloom's learning taxonomy and the e-learning used to cultivate information security culture. They based their study on the Schein's model (artefacts, exposed values, shared assumptions), describing the level of organisational culture. Additionally, the authors stated that for the provision of effective information security culture, it is important to inculcate security knowledge among employees, and this is considered as the fourth layer to the model proposed by Schein (knowledge). The authors attempted to provide effective information security culture based on Schein's model that provided a description of organisational culture rather than information security culture. Hence, the authors added security knowledge as the fourth layer to Schein's model.

In Hogail's (2015) study, the author presented the relationship between knowledge and behaviour in light of information security culture and concluded a positive relationship between the two (security knowledge level and employee behaviour). The study indicates that effective information security culture requires knowledge as the latter can influence information security behaviour and culture.

In related studies, Liebowitz & Wilcox (1997); Zakaria (2006), knowledge-behaviour relationship were evidenced but without further details of such relationship. In a similar study, Rashid et al. (2013) contended that each employee has to be aware of the importance of information security to safeguard the assets of the organisation.

It is crucial to inculcate security knowledge among employees to bring about their effective behaviour and attitude towards information security. In this regard, knowledge and behaviour has to be aligned for effective information security culture within the organisation. Therefore, security knowledge required to influence the employee behaviour are discussed in the following section.

Finally, in order for everyone to perform security tasks efficiently, they need to have security knowledge constructs. To enable employees to internalize and understand the security knowledge constructs, the respective organisation need to establish appropriate internal security awareness and training programs. To focus in details regarding the security knowledge, the following sub sections discuss the importance of security knowledge, then the constructs of security knowledge are presented.

2.4.3 Security Knowledge Construct Required to Influence Employee Behaviour

The related studies concerning security knowledge was gathered for systematic review and analysis using qualitative content analysis. Such analysis uses a subjective interpretation of the text content using a systematic process of classification that codes and identifies themes/patterns within the text.

The thorough review of literature highlighted papers dedicated to determine the security knowledge needed to be provided to employees in order to enhance their behaviour in their interaction with the information assets of the organisation in order to lessen the risks towards such assets. Thus, the following subsections present the security knowledge constructs required to influence employee behaviour in organisation.

2.4.3.1 Knowledge of Security Threat

Employees inside the organisation pose direct or indirect threats to the organisations, with the information assets within vulnerable to cyber-attack that are more often than not, detrimental to the organisational performance. Thus, the inculcation of security knowledge culture among employees will work towards lessening the threats within the organisation and protecting its information assets. Furthermore, it will contribute towards reducing the internal threat posed by insider. Organisational employees always have to be aware of security threats and to achieve this security knowledge has to be instilled in them. The organisation should provide security knowledge in terms of threats to employees to direct and manage their behaviour in their interaction with its assets.

Insider threat stems from an intentional/unintentional action or act of employees in the organisation. On the other hand, external threat is brought about by a third party that executes regular attacks on the organisation through the exploitation of the vulnerabilities that the employees pose. Asset is described as a thing that is valuable to the organisation and this includes information, software, and computer programming, physical device, service, people, skills and experience, and even reputation and image in ISO 27000: 2009..

In the world of technology, the threats are innumerable and are of different types and goals, like vandalism, thievery or extortion. There are many forms of cyber-threats, with some common ones taking the forms of, Malware (malicious software or program that can harm information systems (viruses, spyware, Trojan horses or worms)). These threats are often introduced to the organisations via email attachments or programs downloaded from the Internet. It can also come in the form of Spam (an unsolicited e-mail or undesirable email), spyware (monitoring and spy software), denial of services attacks (making computer resources unavailable to the users), social engineering (obtaining confidential information via interaction or communication with insiders), or phishing (coaxing a user to perform a malicious action). These threats main objectives may be to steal, monitor, change or expose confidential data or assets related to the users.

In organisations, employees often use their smartphones and their mobile phones to maintain their connection with work, along with emails or messages. Moreover, they can work from home by using their laptops and mobile devices courtesy of the pervasive internet technology (Arachchilage & Love, 2014). This compounds the threat from hackers attacking the devices or monitoring them. Employees who use their computers at home are not as likely to be supported and protected by IT infrastructure from cyber-threats and more often than not, they have no security knowledge to safeguard from security threats and attacks.

Moreover, some of the activities that can make the employees' held organisational data susceptible to threats include: (1) browsing unsafe websites, (2) downloading suspicious software, (3) sharing passwords among employees, and (4) disregard for organisation policies. This can be exemplified by some users, who have the habit of writing their passwords on the desk in the office, or on the monitor, and (5) some who leave their computer after work without safeguarding them or following security protocols when it comes to computers and laptops. Others (6) may inadvertently disclose their personal information or that of the organisation to the public through social media, (7) while some others are prone to accessing unsafe websites and go through scam emails or fraudulent websites through which the attack can be initiated. Unsuspecting users have no qualms of entering their user names and passwords, their bank accounts, email accounts or even the organisation's account (phishing) in bogus websites. According to the statistics reported by Google, in 2013, 10,000 websites are daily blacklisted, with vast majority of malware attacks stemming from legitimate sites (Arachchilage & Love, 2014).

Technology Threat Avoidance Theory (TTAT) by (Liang & Xue, 2009) was developed to investigate how to avoid risk of spyware and in a related study, Arachchilage & Love (2014) made use of the model to investigate how employees can avoid phishing. In a similar study, Liang & Xue (2009) mentioned that users are urged to go through security behaviours if they feel the occurrence or presence of the threat and if they cannot avoid it.

Hence, the provision of security knowledge employees is important in this case for the avoidance of threats and for its handling. Organisational employees are also urged to enhance their security behaviour if they are privy to the negative outcomes of the threat on the assets of the organisation.

More specifically, the threat security knowledge covers knowledge of perceived threat, with the latter referring to the level of the individual's perception of the danger and harmful nature of the threat. This knowledge is a combined version of knowledge of threat perceived severity and knowledge of threat perceived susceptibility, indicating that perceived threat covers perceived severity and perceived susceptibility.

In this study, perceived threat is considered to be the level to which an individual perceived the threat as dangerous or harmful, while threat perceived severity is considered to be the negative outcomes if the threat succeeded in attacking. On the other hand, threat perceived susceptibility is considered to be the users' development of threat perception when they are convinced that the IT threat is likely to attack.

The sum up of the TTAT theory is summarized as follows:

- Perceived threat is defined as: *"The extent to which an individual perceives the threat as dangerous or harmful"*.
- Threat Perceived severity means refer to: *"The negative consequences will be serve if they are attacked by the threats"*.
- Threat perceived susceptibility means: *"User develop a threat perception when they believe that the IT threat is likely to attack them"*.

Therefore, the provision of threat security knowledge to employees ensures that they adopt the right action against the threat. According to Arachchilage & Love (2014) ; Liang & Xue (2010), when users are knowledgeable on how to avoid phishing, they will be more confident to adopt the right action towards it.

2.4.3.2 Knowledge of Organisation Information Security Strategy

The organisation information security strategy furnishes the suitable implementation of various information security strategies like plans of actions, policies, objectives, best practices, standards, guidelines and priorities that guide employees to accomplish the goal to safeguard information assets.

Studies in literature have examined the relationship between information security culture and security policies (e.g., (Da Veiga & Martins, 2015; Von Solms, 2006; Von Solms, 2004). More specifically, Da Veiga & Eloff (2010) stated that information security policies is the main component of information security culture.

Organisation information security strategies are employed to facilitate management's adoption of the required direction and support when it comes to information security (ISO: 27001, 2013). Whiteman & Matort (2014) argued that the primary aim of a policy is to drive the decisions, actions and behaviours of employees relating to their interaction with the information assets. Such policy explains employees' acceptable behaviour; for example, the information security policy mandates that laptop must be physically secured at all times. The policy statement aims to direct employee behaviour towards the protection of physical assets and data saved in the laptop. It aims to influence the behaviour of the employee when using the laptop to ensure its safety. The absence of such statement and its enforcement could lead to employees being careless of their laptop's security. In other words, lack of information security component to direct and influence employee behaviour could lead to employees leaving information assets at risk. The negative consequences could lead to an acceptable culture of neglect.

This highlights the importance of the policies to be understandable and acceptable to employees, without challenging them. If the employees are unable to understand the policies or they are not applicable to business, they may steer clear of adhering to them, rendering the information security component ineffective, and laying bare the environment for intentional or unintentional threats. In this case, according to Da Veiga & Eloff (2010), the policy has to be modified to influence and direct the changes needed in the organisational level. In other words, to implement the appropriate information security culture, it is crucial to make sure that information security culture components are identified and implemented to align with organisational culture.

Furthermore, employees would comply with information security policies and practices if they understand the importance of information security in protecting the valuable assets of the organisation against unauthorized and intention misuse by individuals that violate hardware, software, data and computer services (Brady, 2011). This convincing can be done via management support, and the provision of information security programs and information security guidelines that are clear. The level of user awareness can be maximized if the whole organisation practices the recommended information security guidelines, and in turn, this brings about successful implementation of information system security within the organisation.

Studies that dedicated their work to this topic included Cappelli et al. (2009), who stated that a layered strategy comprising of effective policies, guidelines and best practices could be developed to reduce, prevent and detect internal threats. In addition, all of the above measures assist employees in receiving consistent and clear message on what constitutes a violation and the consequences.

In a similar line of study, Siponen et al. (2007) related that in case employees are privy to the information security policy, they are more likely to comply with it. Employees primarily focus on their tasks and jobs and may not be aware of the new policy (e.g., new password requirements) but an effective information security culture ensures that they are made aware of it to protect their computers and sensitive information against threats. In this way adherence becomes a norm.

Practitioners are thus enlightened on how each statement of the organisation's policies, guidelines and strategies has to be positively stated to influence employee behaviour and to uphold information security culture. The objective has to be geared towards instilling security behaviour that protects information assets based on the information security policies, strategies, guidelines and best practices of the organisation. This type of behaviour could entail reporting security incidents, compliance with clear desk policy, or secured disposal of confidential documents.

The above may be exemplified by the confidentiality of passwords and their security from others at all times. This policy directs employees' behaviour to safeguard information assets, facilitate oversight and determine who has control access. This necessitates the employees' obtaining knowledge on the policy and its positive outcomes directed towards protecting assets as a result of complying with the policy. The objective of policy is to influence and to improve the employees' behaviour to ensure the protection of information assets.

In sum, several statements can be developed towards knowledge of organisation information security strategy. These statements are provided in Table 2.1.

Table 2.1 Summary on knowledge of organisation information security strategy statements

Knowledge of Organisation Information Security Strategy Statements	**References**
I know what my organisation's information security strategy is.	(Von Solms & Von Solms 2004; Da Veiga & Eloff 2010)
I know my organisation's information security strategy helps me protect my organisation's information assets in my daily work.	(Von Solms & Von Solms 2004)
I understand the content of information security strategy elements like policy.	ISO/IEC 27001:2013
I know organisation's information security strategy helps me understand what is expected from me as an employee in terms of safeguarding my organisation's information assets.	(Von Solms & Von Solms 2004; Da Veiga & Eloff 2010)
I know that my organisation has developed information security strategies to address the prevention and detection of threats and to respond to them.	ISO/IEC 27001:2013
I know information security requirements to protect information.	(ISO/IEC 27001: 2013)
I am aware of information security policies related to my job such as the password policy.	(Dojkovski et al. 2010)

2.4.3.3 Knowledge of Security Technology

In this study's context, knowledge of security technology refers to the knowledge concerning hardware, software, services, appliances and applications employed by the organisation for the protection of information assets (Hogail, 2015). Disseminating knowledge concerning security technology has a key role in influencing and enhancing employees' behaviour towards protecting the organisation from within. Stated clearly, creating and maintaining an effective information security culture will facilitate the use of various security technology measures. For instance, the antivirus software would be useless to the organisation without its regular update. The holds true with the rest of the security technologies of the company when inappropriately utilized by employees. Developing knowledge of security technology would thus contribute to urging employees' behaviour towards protecting the organisational assets by using technology measures available.

Majority of organisations use different technology control for the protection of information security and for the prevention of threats and security attacks. For instance, the use of firewall, antivirus software, and access management systems which are aimed to safeguard the organisation from threats and attacks and to support its security strategy. Nevertheless, the lack of sufficient knowledge of employees on policy usage of technology may lead to ineffective use of them and may do more harm than good to the organisation. Several statements are developed on knowledge of security technologies they are presented in Table 2.2.

Table 2.2 Summary on knowledge of security technology statements

Knowledge of Security Technology Statements	References
Organisation applies technical security tools and controls in order to preserve information security.	Alhogail, 2015
There is a written policy and guidelines for effective use of information security hardware and software.	
Employees know that the appropriate use of technical controls is vital to achieve information security.	

Help desks and technical staff are prepared to answer and help employees' technical queries and problems.	

2.4.3.4 Knowledge of Legislation, Regulation and National Culture

The organisation’s external environment and national culture significantly impact its information security culture. According to McIntosh (2011), organisations develop their information security assumption on the basis of their social values reflecting the environment. Stated clearly, the legislation, regulation, and national culture of the environment within which the organisation is run have to be considered when designing the organisation’s structure, its information security culture, and security of information assets (Hogail, 2015).

Several studies have been dedicated to this topic and they focused on external factors that influence the information security culture, including national and cultural factors (Alnatheer, 2014; Alnatheer & Nelson, 2009; Connolly & Lang, 2013). Similarly, Dojkovski et al. (2007) highlighted national and ethical culture as well as government legislation as the external factors that have the potential to influence information security culture.

Alnatheer (2014) study provide primary factors namely; corporate governance, legal and regulatory environment and corporate citizens that influence information security culture. The author also indicated that security culture is influenced by organisational culture that is affected by national culture. The study revealed that corporate governance, legal and regulatory environment and corporate citizens all influence an organisation’s information security culture.

National culture has a significant impact on the implementation of information security culture and the behaviour of the employees. Several studies in literature evidenced that the national culture has a significant impact on the implementation of information security culture and the behaviour of the employees (Alnatheer & Nelson, 2009; Connolly & Lang, 2013; Ifinedo,2014; Sherif, Furnell, & Clarke, 2015). Moreover, national culture determines the values and beliefs of the members of the organisation because it naturally influences the viewpoints of the members, their duties and their interaction. In sum, it defines acceptable and not-acceptable behaviour in the organisation. In Ifinedo (2014) study, significant differences were revealed among employees' perceptions of significant computer security threats according to countries. This indicates that when information security culture is designed, national culture has to be taken into consideration due to its influence on employee behaviour. Also, employees should be knowledgeable on legislation, regulation and national culture when it comes to privacy issues and security information laws, as well as intellectual property (in individual and organisation levels). It is also important for information security to be consistent with the security ethics and it should represent the societal values (OECD, 2005).

Moving on to legislation, Al-Hogail (2015) revealed that an effective information security culture within an organisation can be ensured by taking legislation into account in that government regulations concerning information security has to be applied (e.g. copyrights). It is crucial to inform employees of relevant government information security linked to legislation. For instance, they have to be aware of the government monitoring their Internet activities and as such, they should steer clear of visiting restricted sites. On account of the above studies, it is evident that environment factor significantly impacts the developed information security culture of the organisation and they will form the employees' behaviours towards adopting the information systems within.

Al-Hogail (2015) argued that owing to the lack of explicit laws for every ethical situation, the organisation needs to promote ethical responsibilities towards the information assets of the company. This may be exemplified by providing knowledge to employees on taking care of talking about confidential data related to organisation, accessing restricted websites or providing confidential information to such sites. The employee also has to be informed of the privacy laws on privacy of employees, customers and partners' information.

The intellectual property of the organisation should be respected. Employees shall regard the work that they do as organisation's intellectual property. In addition employees should believe that organisation resources such as Internet, e-mail and IT equipment are for work related use and not for personal use.

Several statements are developed regarding the knowledge of legislation, regulation and national culture. The statements are listed in Table 2.3.

Table 2.3 Summary on knowledge of legislation, regulation and national culture statements

Knowledge of legislation, Regulation and National Culture Statements	**References**
Employee know the government regulations regarding information security.	(Martins & Eloff 2002)
Employee are aware of relevant government information security related legislation such as copyrights.	(Martins & Eloff 2002)
Employee are aware of data protection and other relevant legislation and regulations.	ISO/IEC 27001:2013
Employee are aware of the privacy and other relevant legislation and regulations.	ISO/IEC 27001:2013
Employee are aware of government regulations regarding information security.	(Martins & Eloff 2002)
Employee are aware of the importance of the values of intellectual property and copy right laws.	ISO/IEC 27001:2013
Employees believe it is essential to take care when talking about confidential information.	(Martins & Eloff 2002)

2.4.3.5 Knowledge of Security Responsibility

The employees working for the organisation consider the core of its information security culture on account of their important role in protecting information in the information security process (Da Veiga et al., 2007; Eloff & Eloff, 2005; Van Niekerk & Von Solms, 2010). Information security culture primarily aims to facilitate employees' behaviour to work towards the security of information assets, from the top management level to the most menial worker (Paulsen & Coulson, 2011). One of its main goals is to establish that information security is the responsibility of every employee, in that the knowledge of security responsibility culture has to be inculcated in each employee in order to protect the organisation from within. Al Hogail (2015) stressed that information security culture has to consider every human factor to enhance user behaviour. In reality, majority of the employees think that the security of information falls on the IT department's responsibility (Dhillon & Backhouse, 2000), when in fact, employees should be aware of their security related roles and responsibilities and their security behaviour (ISO/IEC27001:2013). The concept of knowledge of security responsibility should be established among employees to have a positive impact on their behaviour.

The responsibility of the top management in this case is to develop security measures for the data protection, to commit towards data protection and information security, and to promote the desired employee behaviour. The management should also obtain requested measures to improve information security strategies in the organisation (Al Hogail, 2015).

Knowledge of security responsibility has to be disseminated among employees through training and awareness in order to achieve the desired employees' behaviour and to improve information security culture (Da Veiga & Eloff, 2010; Safa et al., 2015). Employees have to be educated on their security related roles and responsibilities and trained to behave in a secure manner. They should know how to effectively use information security applications and procedures and what is expected from their interaction with information assets. They should also know what to do when they detect a security breach, and how to disclose threats and risks that can potentially harm information assets. In sum, they should know what to protect, why it needs protection and how they can be a part of the protection (OECD, 2005).

Conversely, the employees should be made accountable for their actions. Actions should be taken against employees who fail to comply with information security requirements. In relation to this, the top management should establish clear policies and formal reward and punitive processes for effective information security culture. Security responsibility knowledge should be promoted within the organisation through reward and deterrent processes and security oversight. There are researchers who have argued that rewarding desirable behaviour and punishing undesirable ones would maximize the adherence of employees to information security needs (Da Veiga & Eloff, 2010; Vroom & Von Solms, 2004).

Several statements are drawn up regarding the knowledge of security responsibility and they are presented in Table 2.4.

Table 2.4 Summary on knowledge of secuirty responsibility statements

Knowledge of Security Responsibility Statements	References
I know that information security is my responsibility in the organisation.	(OECD 2015)
I know that I am responsible for any actions that conflict with information security requirements.	(ISO/IEC 27001:2013)
I know what information security is.	(ISO/IEC 27001:2013)
I know my role with regards to each security policy.	(OECD 2015)
I know what to do when I detect a security violation.	(OECD 2015)
I know what information assets to protect and how I can protect them.	(OECD 2015)
I know that it is essential to protect information assets to achieve business success.	(ISO/IEC 27001:2013); (Da Veiga, 2008)

2.4.3.6 Knowledge of Security Risk

Similar to the previous types of knowledge, this is equally important to drive employee behaviour in their interaction with the organisation's information assets and to understand the risks present in the environment of the information assets. For the establishment of an effective information security culture in the organisation, focus should be placed on risks linked with unmanaged behaviour. It is crucial to educate employees and alert them on the risks and dangers stemming from the environment that surrounds information assets and the risks that may occur when going through an unsecured behaviour within the organisation (Al Hogail, 2015).

Knowledge of security risk aims to promote employees' awareness of security risks and their responsibilities towards security that drive them towards acting in a secure way (Da Veiga & Eloff, 2010; Parsons et al., 2015). Additionally, it assists employees to know, understand and adopt the required precautions and ensure that they possess the required skills for appropriate actions and for the pursuant of secured behaviour (Furnell et al., 2010).

Inculcating knowledge of security risk to employees will help towards safeguarding them, the organisation and the information assets of the organisation. It will also make them aware of the potential risks, which in turn, would affect their behaviour and adopted actions.

In a related study, Thomson et al. (2006) revealed that among the common factors that threaten the security of information within organisations is the employees' erroneous behaviours. The careless and ignorant actions of the employees could lead to information security risks involuntarily. Examples of these actions include an employee retrieves spam email, opens email attachment with virus, or ignore information security policy on external drive use (Dojkovski et al., 2007). Moreover, Employee negligence could risk the organisation network by malware, viruses, worms and Trojans being spread, and seriously expose the whole environment to infection. In addition, when employees attach their personal devices such as USB derives or external hard desks without taking security precautions, there are increased risks of exposing organisation's network to security threats. Majority of employees also use their mobile devices within and outside their workplace and these might contain confidential work-related data, which could be unintentionally exposed to risks when such devices are lost or stolen. Da Veiga (2016) stated many employees carry mobile device outside their workplace containing sensitive work related information which could expose data to risks when lost or stolen.

Other behaviours that could risk employees and their data include downloading suspicious software, browsing through unsafe websites, sharing passwords, or writing passwords on obvious places in the office such as pasting the password on the monitor screen.

Knowledge of security risk will contribute towards identifying security risks and suitable measures required to minimize the risks, if not to prevent it (Blythe, Coventry & Little, 2015). Providing risk awareness to poor password management is the most common awareness and it allows employees to identify the risks related to using poor passwords, maintaining passwords for longer periods, disclosing passwords, recycling passwords and writing passwords on obvious places.

With regards to training awareness, training will help raise the security awareness and decrease accidental, security risk or malicious threats to the information assets. Training should be done on continuous bases to improve the skills and knowledge base that each employee needs when interacting with information. Emerging risks are arising from the dynamically changing environment. This necessitates the organisation's investment in the generation of regular proclamations and reports on information security risk via communication channels among employees. Surveyed employees indicated the use of e-mail, newsletters, digital signage, intranet, posters and workshops to generate regular reports that are security-risk related (Ben-Asher & Gonzalez, 2015; Chen, Ramamurthy & Wen, 2015). Several statements are drawn up regarding knowledge of security risk that are presented in Table 2.5.

Table 2.5 Summary on knowledge of security risk statements

Knowledge of Security Risk Statements	**Reference**
I aware that a weak password represents a security risk.	ISO/IEC 27001:2013
I know the risks when opening web links.	ISO/IEC 27001:2013
I know the security risks and dangerous to the information assets in my work environment.	Hall 1998
I know the risk when opening e-mails from unknown senders, especially if there is an attachment.	Da Veiga (2008) (Martins & Eloff 2002)
I know the risk is when sharing passwords between others.	Da Veiga (2008)
I know the risk is when giving out confidential information of visit prohibited internet sites.	Da Veiga (2008)
I know it is essential to take care when talking about confidential information in public places.	(Martins & Eloff 2002a) (Da Veiga & Eloff 2010)

2.5 Security Behaviour

The security of organisation's information is very crucial in the internetwork environment. There are information security threats coming from outside and inside of organisations. One of the highest information security risk to the information systems comes from insiders who violate the organisational information security either with malicious intentions. Thus, the focus of information security studies is now moving towards studying insiders' security behaviour and their impact on information systems (Crossler et al., 2013). Furthermore, the users inside the organisation is considered the weakest link in the information security chain because they are mostly prone to make mistakes or errors that can jeopardize security (Alhogail, 2015).

Most information security breaches are the results of poor information security practices, human mistakes, errors and negligence (Safa et al., 2015) . Hence, understanding insiders' security behaviour and the factors affecting them can help organisations to control the insiders' security behaviour and reduce security incidents (Molok et al., 2013; Alhogail, 2015).

According to Molok et al. (2013), most employees who leaked sensitive organisational information on social media had no intention to cause harm to the organisation and the factors that influenced such behaviour were more unintentional in nature. A study presented by Da Veiga & Eloff (2010) argued that the information security approach in an organisation should be focused on employee behaviour, provided that success or failure on protecting information depends on what employees do or do not do. So the way users behave may stem from perceptions about perceived threats, controls and punishments and about perceived effort as well as environmental factors such as work overload, fatigue and disgruntlement (Kraemer & Carayon, 2007; Kelloway et al., 2010). These factors may contribute to security behaviour that generate vulnerability and breaches, compromising all the information security principles and turning information into useless pieces of data due to their loss of reliability. There are many definitions related to the concept of behaviour found in the literature, and they are listed below:

- (Rashid et al., 2014:339): "Employee behaviour can be defined: as the way of employee behaves in doing their work either in positive way or in negative way".

The employee behaviour in organisation may affect the organisations' information security effectiveness".

- (Milne, Labrecque & Cromer, 2009:450) : "Risky Behaviour can be briefly defined as specific computer-based actions that put people at risk".
- (Ng et al., 2009:817): "Security behaviour will reduce the risk and/or impact of security incidents".
- (Milne et al., 2009:454): "Security behaviour as specific computer-based actions that individuals take to keep their information safe, and protective security behaviours".
- (Warkentin, Straub & Malimage, 2012: 2): Define security behaviour in two category such as: "white hat and/or black hat. Where, white hat is positive behavioural intentions such as individuals' intention to comply with security policies, rather than negative ("black hat") behavioural intentions such as insider abuse or violation of security policies".
- (ISF, 2000:2): "Employees interact with the organisation's systems and procedures, resulting in a specific behaviour ('the way we do things around here')".
- (Martins & Eloff, 2002:206): "The way people behave towards information security in the organisation".

It is evident from the review of the above definitions, there are many terms related to behaviour such as behaviour, security behaviour and risky behaviour. It is clear that all the terms agree together that the behaviour is the secure way, action, interaction or done provided by the insider towards the protection of information and organisation assets. Furthermore, there are studies that categorize the behaviour into intentional or unintentional behaviour that aims to help the organisation to determine the plane, process and strategies towards the intentional or unintentional behaviour in order to create a secure environment in the organisation that aims to protect the organisation's information.

In the study presented by Alfawaz et al. (2010), they have presented patterns of an individual's behaviour with respect to information security practices and call it modes where a mode means a "manner or way of acting". They identified four modes of behaviours: (I) Not knowing-Not doing mode, (II) Not knowing-Doing mode, (III) Knowing-Not doing mode, and (IV) Knowing-Doing mode. Employee's behaviour may change from one mode to another, depending on their organisational role, the state of technology development, and the status and availability of security training.

According to Hogail (2015), the information security culture shall consider each human factor carefully to improve the user security behaviour. The human behaviour will be influenced by four domains of human factors: "preparedness", "responsibility", "management", "society and regulation". According to the result of their study, employees' behaviour was only affected by two factors: if their background education was IT related or if they are working in the IT department. The results revealed that information security knowledge highly affects information security behaviour. This is similar to the findings of (Van Niekerk & Von Solms, 2010) that employees with no security knowledge or skills will not be able to act securely in the desired way. This is also in line with the finding of (Chen, Ramamurthy & Wen, 2015) that employee's awareness impact security culture.

The Information Security Forum (ISF, 2000) explains information security culture by relating it to industrial safety in organisations' where the safety culture is measured by the number of incidents that occur. They argue that information security incidents in an organisation occur as a result of a series of events that compromise the integrity, availability or confidentiality of information. These events relate to the behaviour of employees or their interaction with information and systems. The behaviour of employees is influenced by their values and beliefs with regard to information security on the one hand and by the organisation's policies on the other hand. As such, the behaviour of employees and the number of incidents that occur in the organisation will portray the information security culture of the organisation. To summarize, the Information Security Forum definition focuses on the interaction between employees and the organisation's information assets, resulting in certain behaviour and incidents. When all employees understand this security behaviour, they are more likely to practice it. When these practices become common, they then become a part of the daily work routine. This can then help to develop an information security culture amongst employees in the organisation.

2.5.1 Insiders' Security Behaviour

Insiders (e.g. employees) are known to be the weakest link of information security chain. Hence, understanding the differences types of security behaviour is important because if intentional and unintentional security behaviour is not clearly understood by organisations, the organisations' security strategies may not be effective to combat insider threats (Crossler et al., 2013). Therefore, having a full view of different kinds of insiders' security behaviour can be very helpful for organisations' managers, professional, and others with an interest to assess end-user security behaviour to understand, observe and control such behaviour (Safa et al., 2015; Stanton et al., 2005).

Loch et al. (1992) develops a taxonomy on the threats to information system (IS). In his taxonomy, threats are divided into: external threats (both human and non-human) and internal threats (human and non-human). Loch's model was one of the first models that recognize the human threats to IS.

Warkentin et al. (2012) extended Loch's taxonomy of IS threats by dividing insiders' behaviour into three categories namely: passive (non-volitional, non-compliance), volitional (not malicious, non-compliance) and intentional (malicious and harmful, computer abuse). It is a model to cover all potential insiders' security behaviour. Further the authors' mentions that many studies should be conducted for each category in order to understand insiders' motivations, so that organisations can detect and prevent undesirable insiders' behaviour in early stage. Additionally, Warkentin et al. (2012) emphasizes that each one of these behaviour must be analysed separately with proper methodologies and theories. In addition to this, the security industry Verizon (2014) categorizes the action of insiders to three main classes: firstly, insiders who perform security behaviour deliberately and maliciously, secondly, insiders who perform security behaviour inappropriately (but not maliciously), and lastly, those who perform security behaviour unintentionally. Further, in the study presented by (Barzak, Molok, Talib, & Mahmud, 2017) categorizes the types of insider behaviour to intentional and unintentional behaviour, this help the organisations to identify the strategies that can protected the organisations from inside. Further, in their paper discusses employees' information security behaviour from the perspective of Islam and provides a behavioural framework that is developed based on the combination of Western contemporary studies and the Islamic principles.

Although the above models are considered to be a fundamental to insiders' security behaviour, they do not cover security behaviour of employees that are desired by organisations and the factors that influence such behaviour.

In terms of intentional behaviour, employees are responsible for their actions whether good or bad because they have the intention to perform the behaviour. Intentional security behaviour in the previous studies only describe malicious insiders who have full intention to cause harm to information system. For example, (NCCIC, 2014:1) defines intentional security behaviour as:

"A current or former employee, contractor, or other business partner who has or had authorized access to an organisation's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organisation's information or information systems".

In Colwill (2009), motivation, opportunity and capability are usually the main factors of any insiders' malicious attacks. Motivations usually come from internal while opportunity and capability are given by organisations. There are many motivations for insiders to engage in malicious behaviours. Some do it for personal gain, financial gain, their ego, their friends and others do it because they have the ability to do it (Liu, Wang & Camp, 2009). However, intentional security behaviour can be easily controlled by organisations by observing and studying the factors that encourage malicious insiders to perform such behaviour (Fernando, 2014). Moreover, organisations that encourage the good security behaviour with clear policies and suitable work environment may be able to manage and mitigate malicious insiders' risks (Colwill, 2009).

From other side, there are even misconceptions of unintentional security behaviour in which it is considered as a security behaviour that is done intentionally but it is done without malicious intent. However, the right definition could be that a behaviour that is performed by employees unconsciously, quickly and spontaneously which can be helpful or harmful to organisational information system. This means it happens accidently without their control and intentions. Despite huge coverage of intentional insiders' security behaviour, security studies that focus on unintentional security behaviour are still limited (Alhogail & Mirza, 2014; Cert, 2013).

According to Greitzer et al. (2014); Liu et al. (2009) security incidents caused by insiders are more likely to be unintentional than intentional. They also posit that most of information leakage incidents and other security breaches are resulted from accidental security behaviour and human mistakes that could cause more damage to organisational system. In (Cert, 2013) the major cause of unintentional information security behaviour is the human error. However, there are some factors which affect these errors and mistakes such as organisational processes, security culture, management practices, and security practice (Greitzer et al., 2014; Cert, 2013 & Harrell, 2014).

2.6 Behaviour Theories and Models

The top theories and models addressing the knowledge-behaviour relationship are reviewed under this section to identify the relationship between the two constructs. This, in turn, assists in adapting the model or theory and develops hypotheses regarding the security knowledge and behaviour relationship.

2.6.1 Theory of Planned Behaviour

The Theory of planned behaviour was developed from the Theory of Reasoned Action (TRA) (Ajzen, 1991). Theory of Planned Behaviour (TPB) to explain the influence of attitude to behaviour, subjective norms, and perceived behavioural control upon individual behaviour. The TPB has been widely applied in diverse studies to predict individuals' behaviour. Theory of Planned Behaviour focused on how to enhance the compliance behaviour between the individual through explains how attitude, perceived behavioural control, and subjective norms affect individuals' intention toward particular behaviour (Safa & Von Solms, 2016).

This theory as shown in Figure 2.1 explains relation between attitude and behaviour (Farrior, 2005; Fishbein & Ajzen, 1991).According to the theory of planned behaviour, the change in behaviour depends on the intention of the person. There are two factors that influence intention. One factor is attitude and the other is subjective norms (Farrior, 2005).

So the level of intention towards an action will be higher if the person has a more positive attitude and more of a subjective norm towards the behaviour. For instance, when a person understands that he/she has control over a certain situation, his/her behavioural intentions reflect this understanding as much as his/her beliefs as to the outcome of a certain behaviour.

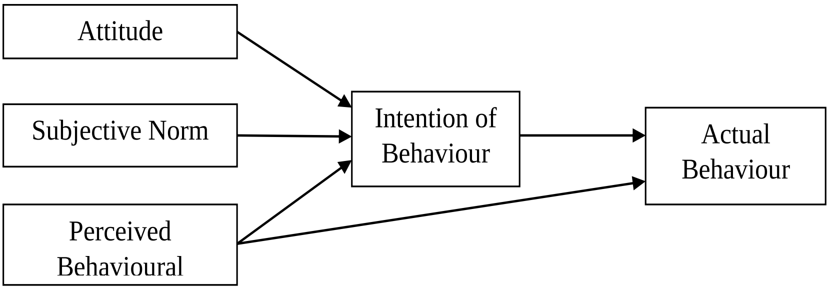


Figure 2.1 Theory of Planned Behaviour Diagram

2.6.2 Protection Motivation Theory

The Protection Motivation Theory (PMT) was developed by Rogers (2002) expanded the health-related belief model in the social psychology and health domains. PMT was developed to help clarify fear appeals. The theory explains that if the threat can be perceived by people as fearful, they will be more cautious and prevent the possible threat (Humaidi & Balakrishnan, 2012). PMT has been noted as one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions (Anderson & Agarwal, 2010). In essence, protection motivation emanates from both the threat appraisal and the coping appraisal. Threat appraisal describes an individual's assessment of the level of danger posed by a threatening event (Woon, Tan & Low, 2005). It is composed of the following two items: Perceived vulnerability and Perceived severity. The coping appraisal is defined as an individual's assessment of his or her ability to cope with and avert the potential loss or damage arising from the threat (Woon et al., 2005). Coping appraisals are made up of two sub constituents - perceived benefit and self-efficacy. The theory argues that individuals are motivated to protect themselves based upon their threat and coping appraisal. An individual’s threat appraisal assesses the perceived susceptibility to the threat and the severity of the consequences. The coping appraisal is their evaluation of the response to the situation and consists of response efficacy and self-efficacy as depicted in Figure 2.2.

Protection Motivation Theory (PMT) which is a risk perception theory exploring an individual’s threat and response appraisal and their motivation to protect themselves. Previous studies have revealed that the motivations associated with individuals' needs and expectations can encourage people to engage in a specific behaviour (Ryan, Lynch, Vansteenkiste & Deci, 2010). Motivation represents the reasons for people's actions, needs, and desires. Motivation defines the direction and the reasons for a particular behavioural pattern. A motive prompts one to behave in a specific manner.

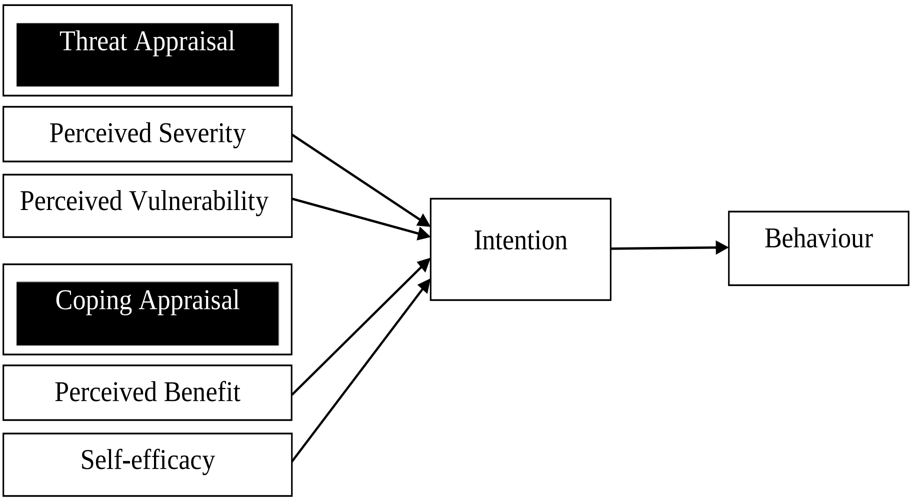


Figure 2.2 Protection Motivation Theory

2.6.3 Health Belief Model

The Health Belief Model is a social cognitive model, first developed in 1952 as a systematic method to explain and predict preventive health behaviour (Rosenstock, 1960). It has been widely applied to all types of health behaviour, such as contraceptive use, diet and exercise. It has also been applied in other diverse areas, such as preventive behaviour against piracy threat facing U.S. firms and emigration intention (Groenewold, de Bruijn, & Bilsborrow, 2006). The model appears to have implications for work motivations as well as a broad range of employee behaviours (Walker & Thomas, 1982).

The Health Belief Model as shown in Figure 2.3, argues that a person's beliefs about a condition determine what he will do about it. It uses two aspects of individuals' representations of health behaviour in response to the threat of illness – perceptions of illness threat and evaluation of behaviour to resolve this threat. Perception of illness threat depends on two beliefs – the perceived susceptibility to the illness and perceived severity of the illness. Evaluation of behaviour depends on the perceived benefits of the health behaviour to prevent the illness and the perceived barriers to performing the preventive health behaviour, thus giving the perceived net benefit (Conner, 2010). The Health Belief Model submits that, anytime there is an increase in an individual's assessed level of risk, there is an increase in the likelihood that the individual will adopt recommended prevention behaviours.

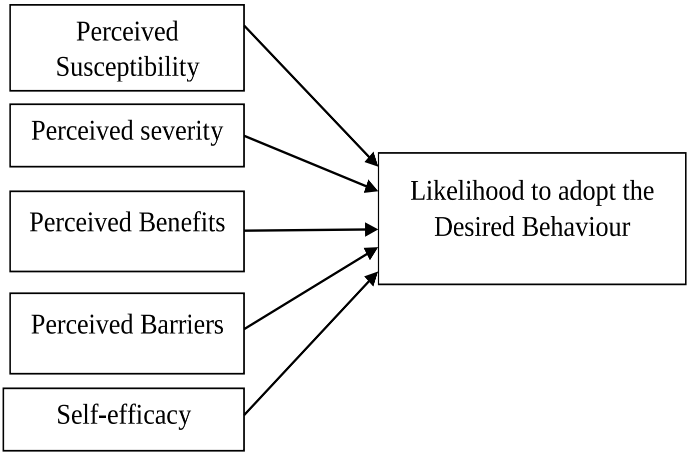


Figure 2.3 Health Belief Model

2.6.4 Theory of Bounded Rationality

In the Theory of Bounded Rationality (Simon, 1955), individuals may lack knowledge or may be faced with ambiguity or uncertainty, which could influence their attitude, and hence, behaviour may not be optimal (Jones, 1999). In addition, although employees may try to make good decisions, it is often impossible to take into account all of the relevant information to make an optimal or rational choice (Huber, 1981).

According to Simon (1955), individuals do not have access to all information when making decisions, nor the capability to assess it. In other words, rational decision-making theories do not describe the way that humans think, but the way they should think to make the best decisions.

2.6.5 Human Behaviour Theory

In the Human behaviour theory, the individual's attitude is the key element of the individual's intention to perform the actual behaviour (Alumaran, Bella & Chen, 2015). Human behaviour theory, which is based on the employees' attitudes towards information security, which play a major role on the individuals' use and misuse of information in health services. The intention to use the hospital information such as patient's information can lead to the actual use of the information.

2.6.6 KAB Model

In KAB model (Knowledge – Attitude – Behaviour) (Kruger & Kearney, 2006) as shown in Figure 2.4, where knowledge affects the attitude of an individual towards a particular behaviour, and in turn, an attitude enhance the desired behaviour. The model sheds light on the role of knowledge in behavioural change and the knowledge accumulation, with such knowledge accumulation leading to changes in attitude, and ultimately, changes in behaviour. In other words, with the accumulation of knowledge in a certain behaviour, changes eventually occur in attitude that will increasingly change the behaviour in question.

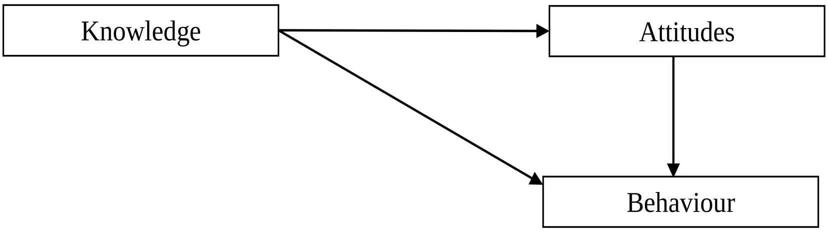


Figure 2.4 KAB Model

2.6.7 Summary of Behaviour Theories and Models

In summary, Table 2.6 summarizes the theories and models identified in literature to address the knowledge-behaviour relationship and their description.

Table 2.6 Theories on Relationship between Behaviour and Knowledge

Author's Names	Theory/ Model Name	Summary
(Ajzen, 1991)	Theory of Planned Behaviour (TPB)	An extended version of TRA. The model focuses on perceived behavioural control and subjective norms and their influence on individuals' intention to a given behaviour to explain compliance behaviour (Focused on Attitudes).
(Rogers, 1983)	Protection Motivation Theory	Individuals are motivated to safeguard themselves on the basis of their appraisal of a threat, appraisal of how they cope, perceived susceptibility, perceived vulnerability and severity of the outcomes.
(Rosenstock, 1960)	Health Belief Model	Beliefs of an individual regarding a condition will determine his behaviour towards it. The model uses two aspects of specific behaviour representation in response to the severity of a threat namely, perceptions of the threat and the evaluation of behaviour to resolve such threat.

(Simon,1955)	Theory of Bounded Rationality	Individuals may lack knowledge or may face ambiguity or uncertainty, and this may be affected by their attitudes, in which case optimal behaviour may be elusive.
(Follett, 1930)	Human Behaviour Theory	Individual attitude is the major element of the intention of an individual to behave and to display actual behaviour.
(Kruger & Kearney, 2006)	KAB model (Knowledge-Attitude- Behaviour)	The model focuses on the relationships among the constructs of knowledge, attitude and behaviour. knowledge influences an individual's attitude towards a specific behaviour, and a positive attitude is generally associated with better behaviour

The theories listed in Table 2.6 have been studied in literature extensively with most of them focused on improving behavioural compliance via attitudes and intention of attitudes. Other studies addressed individual's motivation to protect from or avoid threats based on their severity, susceptibility or probability.

In this study, the KAB model has been adopted in this study that matches the relationship assumptions between knowledge and behaviour is the model. In section 5.2 justifies the adoption of KAB and discuss the association among the constructs of knowledge, attitude and behaviour.

2.7 Related Works on KAB model (Knowledge – Attitude – Behaviour)

This section aims to explore and understand KAB model (Knowledge, Attitude and Behaviour) and discuss the relation between knowledge, attitude and behaviour. Firstly, it produce introduction into KAB model. Review on use KAB models in information security. Next, discuss the adaptation of KAB model to include security knowledge constructs to influence the behaviour in this research. Then discuss the proposed variables in knowledge, attitude and behaviour in KAB model.

2.7.1 Overview of KAB model

The Knowledge-Attitude-Behaviour (KAB) model, which is developed by (McGuire, 1969) as a health promotion campaigns to change people's lifestyles (behaviour), or to prevent negative lifestyles in order to improve their long-term health status. KAB model frequently used to assess behaviour change, has been proposed as a way of explaining the role of knowledge. It explains that a person's knowledge directly affects attitudes, and indirectly affects behaviours through attitudes (Bettinghaus, 1986). McGuire's (1969) developed information processing model of attitude change and then examined in terms of knowledge from social psychology and communication research and its potential relevance to health promotion campaign.

McGuire has suggested a persuasion matrix as shown in figure 2.5, which is a way of conceptualizing the change process and understanding the complexities of the relationships between outcomes (changes in knowledge, attitudes, and behaviour), and inputs (Flay, DiTecco, & Schlegel, 1980). This matrix includes elements related to communication process such as source, message, channel, receiver and destination as communication components. It is suggested that any review or evaluation of the potential effectiveness of mass media programs needs to consider each of the above elements of the communication process. There are six steps in the stochastic process of general attitude change which are exposure, awareness, knowledge, attitude, persistence and behaviour. It is generally assumed that this matrix helps to achieve belief changes and this will automatically lead to attitude and behaviour change (Flay et al., 1980).

Generally McGuire's model offers a good paradigm for the planning and assessment of mass-communication in health-promotion campaigns. However, certain challenges might be a rose concerning the validity of the assumption that changes in knowledge and beliefs will automatically lead to changes in attitude and ultimately behaviour. This is directly relevant to the appropriateness and comprehensiveness of the model for assessing and planning health promotion strategies based on mass communication approaches (Flay et al., 1980).

Independent Variables Dependent Variables	Source	Message	Channel	Receiver	Destination
1) Message Presentation →Exposure					
2) Attention → awareness					
3) Comprehension → Knowledge					
4) Yielding → Beliefs / Attitudes					
5) Retention → Persistence/ Maintenance					
6) Action → Behaviour					

Figure 2.5 McGuire's persuasion matrix.

2.7.2 Relationship between Knowledge, Attitude and Behaviour in KAB Model

Kruger and Kearney [5] developed a prototype model based on techniques borrowed from the field of social psychology that proposes that learned predispositions to respond in a favourable or unfavourable manner to a particular object have three components: affect, behaviour and cognition. These three components were used as a basis and the model was developed on three equivalent dimensions namely what does a person know (knowledge); how do they feel about the topic (attitude); and what do they do (behaviour) (Kruger & Kearney, 2006). Thomson & von Solms (1998) argued the social psychological principles could be utilized to improve the effectiveness of an information security awareness program.

Kruger & Kearney (2006) developed a prototype for measuring information security awareness using knowledge, attitude and behaviour (KAB). The underlying theory for KAB is that it seeks to understand the relationship between these three components, suggesting that as knowledge accumulates in a relevant behaviour, say for example in information security, health, education, it will eventually initiate changes in attitude that will gradually initiate the change in behaviour. In KAB model (Knowledge – Attitude –

Behaviour) (Kruger & Kearney, 2006) as shown in Figure 2.6, knowledge refers to the focus of what an employee knows; attitude focuses on what an employee think; and behaviour is about what an employee does (Kaur & Mustafa, 2013).

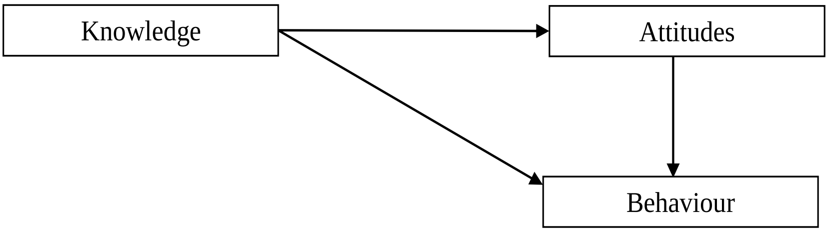


Figure 2.6 KAB Model

The KAB model posits that knowledge is gathered over time of a relevant behaviour; for instance, in different fields such as information security, health, environment, education information, among others, initiate change in attitude. The model sheds light on the knowledge role in behavioural change and the knowledge accumulation, with such knowledge accumulation leading to changes in attitude, and ultimately, changes in behaviour.

2.7.3 The Use of KAB Models in Information Security and KAB Model Variables

The related studies concerning the use of KAB model in information security was gathered using systematic review and analysed using qualitative content analysis. Such analysis uses a subjective interpretation of the text content using a systematic process of classification that codes and identifies themes or patterns within the text.

A thorough review of literature highlighted papers dedicated to KAB model in information security that discuss use of KAB model, the development of KAB model or the proposal of model to enhance the KAB model in information security. All the studies that used KAB model in order to examine the relationships between knowledge, attitude and behaviour are in the field of information security awareness.

Kruger & Kearney (2006) proposed KAB model for assessing information security awareness in an international mining company. They measured the effectiveness of information security awareness program on the basis of knowledge, attitude and behaviour. This aims to ensure that their employees are informed and aware of security risks, thereby protecting themselves and their profitability. The proposed tool was based on techniques borrowed from the field of social psychology that proposes that learned predispositions to respond in a favourable or unfavourable manner to a particular object have three components: affect, behaviour and cognition. These three components were used as a basis and the model was developed on three equivalent dimensions namely what does a person know (knowledge), how do they feel about the topic (attitude) and what do they do (behaviour).

Kruger & Kearney (2006) focused on the following six risk categories: always adhere to company policies, keep passwords and personal identification numbers secret, use e-mail and the Internet with care, be careful when using mobile equipment, report incidents like viruses, thefts and losses and be aware, all actions carry consequences. As a first classification of what to measure, it was decided to measure the three dimensions which are: knowledge, attitude and behaviour. Each one of these dimensions was then subdivided into the six focus areas and on which the awareness program was based. Such model of divisions and subdivisions aim to measure information security awareness based on the proposed KAB model.

Khan (2011) proposed a model which is the integration of knowledge-attitude-behaviour (KAB) with factors of theory of planned behaviour TPB to influence the employee behaviour. The proposed model includes knowledge, attitude, norms, intention of behaviour and actual change in behaviour. The KAB model, by itself is not sufficient to bring change in attitude and behaviour for long term. In order to understand the change in attitude and behaviour and how a change in attitude leads to change in behaviour he borrowed some elements from Theory of Planned Behaviour (TPB). This theory explains relation between attitude and behaviour and includes both the direct attitude-behaviour path as well as an indirect attitude-intention-behaviour path. The proposed model takes the knowledge attribute from the KAB model, attitude and social norms from the theory of planned behaviour to achieve the desired change in behaviour. Finally, the author suggested the following methods for effectiveness of information security awareness namely, educational presentation, e-mail messaging, group discussions, newsletter articles, video games, computer-based training and poster. The author concluded that providing information security awareness campaigns based on the proposed model have the ability to change user's behaviour and hence raise user's information security awareness.

Kaur & Mustafa (2013) reports awareness of information security at a small and medium enterprise in Malaysia based on KAB model. To establish the relationship between knowledge, attitude and behaviour in information security awareness among the employees in terms of availability, confidentially and integrity, a survey questionnaire was used to collect data. The findings revealed that attitude and behaviour have significant influence on confidentiality, integrity, and availability of business information while knowledge was found to be not significant to availability.

Parsons et al., (2014) developed a tool based on KAB model to produce an empirically validated instrument, known as the Human Aspects of Information Security Questionnaire (HAIS-Q). This tool includes specific items to measure each factor in KAB model, for example, organisational factors are measured via organisational and security culture, subjective norms, rewards and punishments in order to develop KAB model. This tool could be used to measure employee knowledge, attitude and behaviour to provide management with a benchmark. The aim of the paper is to outline the development of HAIS-Q and to examine the relationships between knowledge of policy and procedures, attitude towards policy and procedures and behaviour when using a work computer. They used the model in seven focus areas: internet use, email use, social networking site use, password management, incident reporting, information handling and mobile computing.

Mäeses, (2015) proposed an evaluation method for human aspects of information security that uses an online framework in order to give employees fast and personalized feedback on their self-report based on KAB model across different focus areas. An empirical study is performed to aid in validating the proposed evaluation method for human aspects of information security. In this study, knowledge, attitude and behaviour in KAB model are measured in seven focus areas. These areas are: password management, e-mail use, internet use, social networking site use, incident reporting, working remotely, information handling.

Chmura (2017) provided methods of training awareness in the field of information security that aims to mitigate the risks of information security. The aim of the study was to present the essence and importance of information security awareness as well as to analyses selected methods used in forming the employee awareness in information security. The author suggested methods for forming security awareness for employees namely, traditional methods, educational game and films, and internet method. The author concluded that information security awareness is a dynamic process, dependent on ever-changing threats. It is therefore considered that any safety awareness program should be subjected to continuous monitoring, thus forming an integral part of the company's culture. Finally, the author suggested the use of KAB model to explain the role of knowledge in behaviour change. The analysis of study shows that the increasing employee awareness of information security is largely dependent on the method of providing knowledge. In addition, the literature studies have confirmed that awareness-raising methods and techniques, such as trainings and communication, are effective in enhancing user safety knowledge, including promotion of appropriate attitudes and behaviour.

Gandhi (2017) evaluated the information security awareness for informatics student based on KAB model in order to guide university to formulate information security awareness program for their students based on the result of this study. In this study modifies six focus areas that adopted from Human Aspects of Information Security Questionnaire (HAIS-Q), in which each sub-focus area is expanded into three criteria using Knowledge- Attitude-Behaviour based on KAB model. The author found that there is a positive relationship between knowledge, attitude and behaviour with respect to ISA measurement.

Mustafa et al. (2019) proposed a model called as enhanced Knowledge-Attitude-Behaviour (KAB). The knowledge in KAB model was enhanced to include an e-learning element. This is to investigate the function of e-learning in enhancing the awareness level for simple and faster understanding. E-learning element also includes presentations with video clips on spear phishing, available online through open learning and phish awareness blog for enhance self-study by user. The name of the developed model is ISA KAB model

(Information Security Awareness, knowledge, attitude and behaviour) model. The aim of the model is to raise the awareness level among students and to investigate the awareness level of phishing attacks on the targeted group of vocational students.

Table 2.7 summarizes the studies that utilized KAB model for measuring information security awareness.

Table 2.7 Studies that utilized KAB model for measuring information security awareness

Authors	The use of KAB Model
Kruger & Kearney (2006)	Proposed KAB model for measuring information security awareness in an international mining company. Measured the effectiveness of information security awareness program on the basis of knowledge, attitude and behaviour in KAB model.
Khan (2011)	Proposed a model with integration of knowledge-attitude-behaviour in KAB model with factors of theory of planned behaviour TPB to influence the employee behaviour. The proposed model includes knowledge, attitude, norms, intention of behaviour and actual change in behaviour.
Kaur & Mustafa (2013)	Evaluate the awareness of information security at a small and medium enterprise in Malaysia based on KAB model.
Parsons et al., (2014)	Developed a tool based on KAB model namely, Human Aspects of Information Security Questionnaire (HAIS-Q) that that can be used to measure information security awareness.
Mäeses, (2015)	Proposed an evaluation method for human aspects of information security that uses an online framework in order to give employees fast and personalized feedback on their self-reported based on KAB model.

Chmura (2017)	Provided methods for training awareness in field of information security then used KAB model to measure the security training awareness.
Gandhi (2017)	Evaluated the information security awareness for informatics student based on KAB model in order to guide university during strategies formulation for students ISA.
Mustafa et al., (2019)	Proposed a model called enhanced Knowledge-Attitude-Behaviour (KAB). The knowledge in KAB model has been enhanced to include the elements of e-learning knowledge. That aim to investigate the role of e-learning knowledge in enhancing the security awareness programs between the employees.

Based on the literature review conducted, all the studies summarized in Table 2.7 used KAB model to measure information security awareness among the employees in terms of knowledge, attitude and behaviour. It is clear from the table that the studies can be divided in two groups.

The first group (e.g., Khan (2011); Mustafa et al. (2019)) enhanced KAB model by including items from other theory such as theory of planned behaviour. This aims to influence the behaviour in KAB model. So, the enhanced model includes knowledge, attitude, norms, intention of behaviour and actual change in behaviour (Khan, 2011). Furthermore the knowledge in KAB model has also been enhanced to include the elements of e-learning knowledge. This aims to investigate the role of e-learning in enhancing the security awareness programs for employees (Mustafa et al., 2019). On other hand, the second group (e.g., Kruger & Kearney (2006); Kaur & Mustafa (2013); Parsons et al., (2014); Mäeses, (2015); Chmura (2017); Gandhi (2017)) suggested many methods to enhance information security awareness, and then use the KAB model to measure the effectiveness of information security awareness program between the employees on the basis of knowledge, attitude and behaviour in KAB model.

Based on the literature review conducted on the use of KAB model in information security, the KAB model is mainly used to measure the effectiveness of information security awareness programs. In a recent work done by Mustafa et al. (2019), the knowledge component of the KAB model is enhanced to include the elements of e-learning so that the effectiveness of using e-learning can be measured. However, given that there are many different types of security knowledge, it is not yet known which of them can influence the employee's security behaviour and in what way the behaviour is influenced by the knowledge. This has not been explored in any of the previous research works on the use of KAB model in information security. It is hypothesized that different types of security knowledge will have different influence on an employee's security behaviour and therefore the KAB model as proposed by Kruger & Kearney (2006) needs to be extended to represent the relationship between the security knowledge construct and behaviour. In particular, the knowledge component of the KAB model needs to be extended to include the relevant security knowledge constructs that can be included in an information security awareness program so that the impacts of each type of knowledge on the attitude and behaviour of the employee can be measured.

Based on the review that has been conducted on the related papers on KAB model, many variables has been identified from these papers. These variables are identified and analysed using content analysis in knowledge, attitude and behaviour in KAB model. The following table present the variables for each element in KAB model.

Table 2.8 Summary on varibles element of knowledge, attitude and behaviour in KAB model

Knowledge	Attitude	Behaviour

a. Knowledge b. Understanding c. Strengthen Security d. Security Experiences e. Perceived Support f. Define/State g. E-Learning	a. Positive Attitude in Handling Knowledge b. The Way of Thinking c. Acceptable Action Level d. Faster Respond e. Adhere To Action f. Unaware / Careless g. Affective- Feeling Like/Emotion h. Recognizing	a. Habits b. Actual Action c. Prompt /Reflect Decision Making d. React to Situation e. Physical Action f. Psychomotor Skills

2.8 The Interaction Model between Knowledge, Attitude and Behaviour to Reduce Internal Security Incidents

An information security culture develops due to the information security behaviour of employees, in the same manner that an organisational culture develops due to the behaviour of employees in the organisation (Da Veiga & Eloff, 2010; Da Veiga et al., 2007; Martins & Eloff, 2002). An information security culture is therefore based on the interaction of employees with information assets and the security behaviour they exhibit within the context of the organisational culture in the organisation. Information security culture is therefore defined as the attitudes, assumptions, beliefs, values and knowledge that employees use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (Da Veiga, 2008).

Furthermore, employee behaviour can be defined: "as the way of employee behaves in doing their work either in positive way or in negative way" (Rashid et al., 2014). The employee behaviour in organisation may affect the organisations' information security effectiveness.

In the study presented by Da Veiga & Eloff (2010), they specify the interaction between behaviour and information security culture through a model which describes the interaction between information security components such as a policy and the behaviour of employees that eventually has an impact on the resulting information security culture.

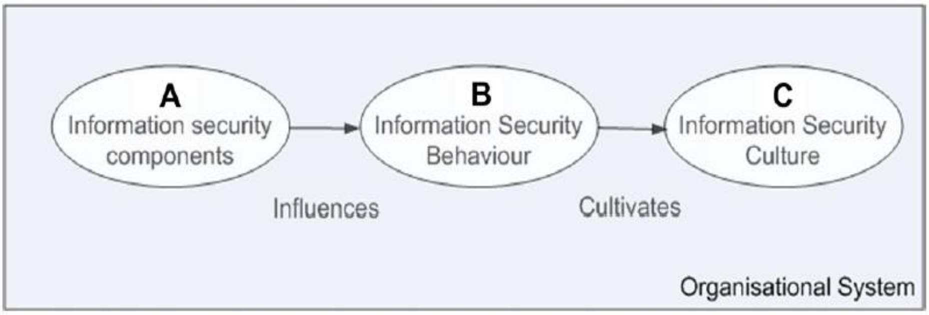

A
Information security components
B
Information Security Behaviour
C
Information Security Culture
Influences
Cultivates
Organisational System

Figure 2.7 Influencing information security behaviour and cultivating an information security culture(Da Veiga & Eloff, 2010)

Fig. 2.9 illustrates that information security components (part A in figure 2.7), are implemented in the organisation. These components can be seen as the input that influences information security behaviour in the organisation (part B in figure 2.7). Implementing the information security components will influence the interaction of employees with information assets, and employees subsequently exhibit certain behaviour referred to as information security behaviour.

The objective is to influence employees' security behaviour that is conducive to the protection of information assets based on security knowledge constructs as presented in this study. Such behaviour could involve the reporting of security incidents, adherence to a clear desk policy, manage the password policy or the secure disposal of confidential documents. In time, this security behaviour evolves as the way that things are done in the organisation and an information security culture is therefore established (cultivated) (part C in figure 2.7) A culture is thus promoted in which information security is accepted as the way things are done.

To illustrate the interaction between A, B and C in figure 2.7, the following example is used. By implementing the security knowledge constructs on the employees in the organisations, for example knowledge regarding the information security policy as one of the organisation information security strategy components (KOISS). According to Whitman & Mattord (2011) the objective of a policy is to influence the decisions, actions and behaviours of employees. It further specifies what behaviour is regarded as acceptable and what is not. For instance, the information security policy states that a laptop must be physically secured at all times (part A in figure 2.7). The statement in the policy is aimed at directing employee behaviour to protect both the physical asset and the data saved on the laptop. The objective is to influence the employee's behaviour when interacting with the laptop to ensure its safeguarding (part B in figure 2.7). In time, this security behaviour evolves as the way that things are done in the organisation and an information security culture is therefore established (cultivated) (part C in figure 2.7). Without this statement and the enforcement thereof, employees could leave their laptops unsecured. Therefore, without knowledge of the information security components that aims to direct and influence employee behaviour, employees could interact with information assets in ways that would introduce risk. In time, this potentially harmful behaviour could unfortunately give rise to a culture where neglect is regarded as acceptable.

To cultivate an acceptable level of information security culture among the employees, organisations should ensure that a comprehensive and adequate set of security knowledge constructs is implemented. This set of security knowledge constructs aids in addressing threats on the human, process and technical levels that would help to direct the employee behaviour in order to establish an acceptable appropriate security perception between the employees within the organisation (Alhogail, 2015). Organisations should furthermore ensure that employee interaction is in line with the requirements of the security knowledge constructs. These requirements could relate to actions such as making back-ups to the server on a daily basis, password protect information on removable media or the deletion of unsolicited e-mails with attachments. Employees must have sufficient security knowledge level concerning their roles and responsibilities in the process of security systems. Also, security knowledge has to be developed in day-to-day activities supporting the business activities as part of the culture of the organisation. In other words, information security should become a natural practice in day-to-day employee activities. Cultivating each employee's security knowledge plays a crucial role in bringing about their desired behaviour and to find an appropriate security perception between the employees.

It is evident that if employees can interpret or understand security policy and the relevant documents, they can behave in accordance with official security policies. They perform security activities accordingly and their security behaviours would become visible. Visible security behaviours are important because they can be good examples of security practices which can inspire everyone in the organisation. In an ideal situation, once employees know how to perform security activities in their daily work routine, then security practices can become entrenched within the organisation, which in turn can help to cultivate an appropriate information security culture amongst employees.

Furthermore, when people understand the importance of these security knowledge constructs, how to use it, and where to report if incidents occur, they can help reduce the internal security incidents within an organisation and at the same time can increase the organisational effectiveness and protect the organisational assets. This is supported by (Whitman & Mattord, 2013), where they conclude that security awareness, training, and education program can improve employees' behaviour in handling information properly, and at the same time make employees accountable for their actions. Therefore, the organisations should provide awareness training on these security knowledge constructs (knowledge of security threat, knowledge of organisation information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility and knowledge of security risk), that aim to guide the employee behaviour when interacting with information assets in order to protect the organisation information assets. Which in turn can help to cultivate an appropriate security behaviour amongst employees.

According to Al-Awadi & Renaud (2007), awareness and training program is one of the success factors in information security implementation in organisations where it would give a significant impact in helping organisations to achieve organisation's information security effectiveness. Hagen & Albrechtsen (2009) point out that information security awareness has a significant effect in improving user's security knowledge and behaviour. Once people are aware of information security, they will know which behaviour should be applied and practiced in order to minimize the number of internal security incidents in an organisation. Furthermore, according to Colwill (2009) having information security awareness may change people's behaviour and also enhance the level of trust between an employer and his employees.

This research study is concerned with guiding organisations and professionals in influencing the behaviour of organisation employee that ensures that employees have the security knowledge required to guide their behaviour when interacting with information assets. These set of security knowledge constructs (knowledge of security threat, knowledge of organisation information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility and knowledge of security risk) can be grouped into categories of security knowledge in part (A- see the figure 2.7) that are implemented by the organisations on the individual, groups or organisation level tier. The objective of implementation of these security knowledge for each tier help to influence the employee's behaviour when interacting with the organisation information assets to achieve (part B in figure 2.7). In time, as such, security behaviour is influenced and exhibited on each behavioural tier this security behaviour evolves as the way that things are done in the organisation and an information security culture is therefore established (cultivated) to create a suitable appropriate security behaviour between the employees, so (part C in figure 2.7) is achieved). When all employees understand these security behaviour, they are more likely to practice it. When these practices become common, then they become a part of the daily work routine. This can then help to develop an information security culture amongst employees in the organisation. Figure 2.8 summarizes the interaction between knowledge, attitude and behaviour in KAB model to create an appropriate employee security behaviour which can be used to minimize internal security incidents. When everyone performs security practices efficiently, internal security incidents can be reduced. It must be emphasized that an appropriate employee security behaviour can help to increase an organisation's ability to protect the information assets from inside.

It's clear from the above, this study focuses on security knowledge required to influence the employee behaviour in order to minimize the risk posed by insider with in organisations. These security knowledge constructs can be provided by a training awareness program for employees in organisations.

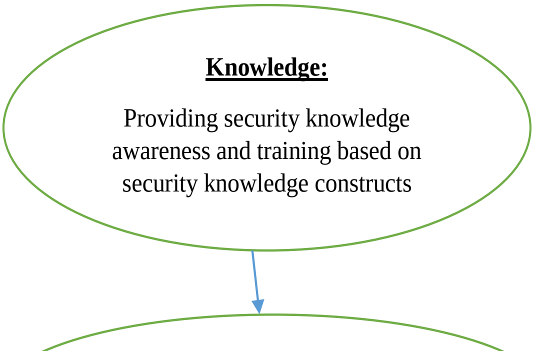

Knowledge:
Providing security knowledge awareness and training based on security knowledge constructs

Figure 2.8 The realatioship between Knowledge, Attitude and Behaviour to Reduce Internal Security Incidents

2.9 Summary

This chapter contains the major issues related to information security culture including its definitions and related literature in the domain. A thorough review of literature revealed a relationship between human knowledge and behaviour. The security knowledge required to improve employee behaviour is identified in this chapter. Moreover, the relation between information security culture and organisation culture presented in this chapter, also the relation between behaviour and information security culture also presented. In this chapter examines how security knowledge enhances employee behaviour in interacting with the information assets of the organisation. Furthermore, the relationship between security knowledge constructs, behaviour and information security culture are explained. Many risk posed by the human factor also presented in this chapter. A discussion on KAB model including, introduction to KAB model, review on studies that use KAB model to enhance and develop KAB model in information security, adapting KAB model and propose the variables in element of KAB model also discussed in this chapter.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This chapter provides a discussion of the research methodology employed in this study and their details. Several methodologies have been used in many prior studies, with each illustrating various aspects of the complete picture. Accordingly, this chapter begins with an overview of the methods used in this research covering research design, addressing the reason and justification behind using the mixed-method approach in this study. The chapter then presents the research model and the development of hypotheses. This is followed by a discussion of the research methods involving quantitative and qualitative data collection methods and the selected analysis method. Finally, the chapter ends with the chapter conclusion.

3.2 Research Operational Framework

The methods and procedures are included in the research operational framework in order to help the researcher to conduct the research. The research operational framework is depicted in Figure 3.1, which is based on Creswell (2013) research method. Based on this, the research methods are mainly focus to address the research questions, and then to achieve the research objectives. This research study consists of five main phases as shown in Figure 3.1.

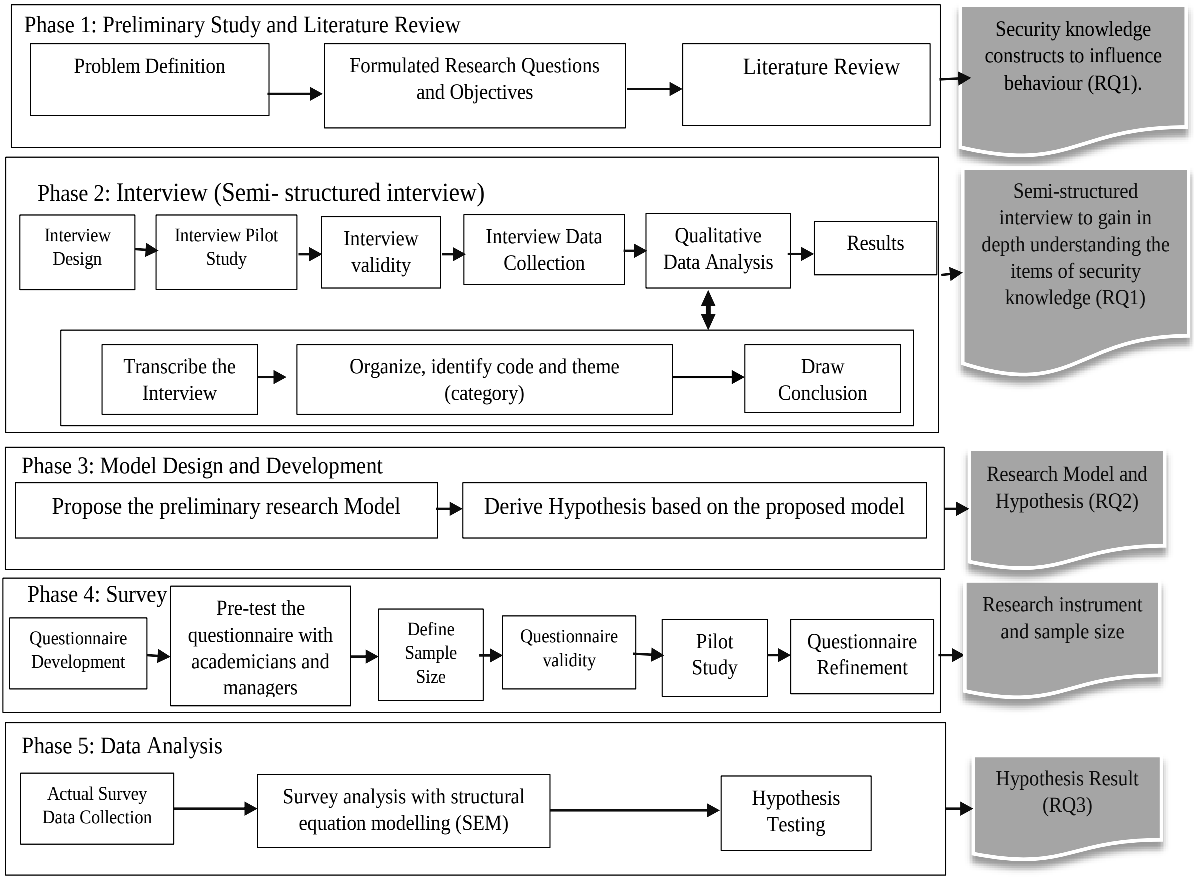

Phase 1: Preliminary Study and Literature Review
Problem Definition
Formulated Research Questions and Objectives
Literature Review
Security knowledge constructs to influence behaviour (RQ1).
Phase 2: Interview (Semi- structured interview)
Interview Design
Interview Pilot Study
Interview validity
Interview Data Collection
Qualitative Data Analysis
Results
Transcribe the Interview
Organize, identify code and theme (category)
Draw Conclusion
Semi-structured interview to gain in depth understanding the items of security knowledge (RQ1)
Phase 3: Model Design and Development
Propose the preliminary research Model
Derive Hypothesis based on the proposed model
Research Model and Hypothesis (RQ2)
Phase 4: Survey
Questionnaire Development
Pre-test the questionnaire with academicians and managers
Define Sample Size
Questionnaire validity
Pilot Study
Questionnaire Refinement
Research instrument and sample size
Phase 5: Data Analysis
Actual Survey Data Collection
Survey analysis with structural equation modelling (SEM)
Hypothesis Testing
Hypothesis Result (RQ3)

Figure 3.1 Research Operational Framework

3.2.1 Phase 1: Preliminary Study and Literature Review

Phase one of the current research includes: 1) problem definition, 2) formulating of research questions and objectives and 3) reviewing the literature on Information Security Culture approaches in general and the approaches focused on security knowledge, identifying the security knowledge constructs to influence employee behaviour, and also to investigate the relationship between knowledge and behaviour in information security culture. Once a researcher decides the area to conduct his study, it is required to search for relevant information sources that help to determine what is already done about the topic and what the current situation of the topic is. In many cases, a researcher may find certain aspects that need further exploration by reviewing what has already been written on the topic.

Defining the research problem has begun during the phase of preliminary study and literature review. The previous studies helped the researcher to look at an area where previous researchers generated some interesting results, but never followed up and not fully explored. The researcher conducts this by going into the subject in-depth, by deciding what is needed to be researched and why. The study starts with putting the problem in a wider perspective to highlight the issues which are important and should be taken into consideration. After identifying the gap in the previous studies, research questions formed which then lead to the research objectives.

The input of this phase involves the literature review related to the topic, which helped in the setting of the problem of the study. The outputs from this phase are research problems, research questions, research objectives, and the identification of security knowledge constructs that help to improve employee behaviour as well as review of related literatures. The discussion details of this phase are categorized into Chapters I and II, which contributed to the achievement of the first objective.

3.2.2 Phase 2: Interview

The main aim of this phase is to ensure and explore the security knowledge constructs required to influence employee behaviour. Semi- structured interview has been conducted with group of information security experts from different perspective to gain an in depth understanding the items and variables of security knowledge constructs to influence the employee behaviour. The detailed discussion of this phase is contained in chapter Four, which also helped in the achievement of the first objective.

3.2.3 Phase 3: Model Design and Development

A review of related literature has been conducted to focus on the models and theories that identified the relationship between knowledge and behaviour. One of the most suitable model to represent the relationship between knowledge and behaviour is KAB model (Knowledge- Attitude- Behaviour). The aim of using the KAB model is to determine the impact of each security knowledge constructs to employees behaviour. The output of this phase is the adopted research model, as well as the research hypothesis where a total of 19 hypotheses were derived. The detailed discussion of this phase is contained in Chapter Five, which also helped in the achievement of the second objective.

3.2.4 Phase 4: Survey

In the survey phase, the main issue is related to the data collection techniques for a thesis. First, a draft tentative questionnaire is designed based on the initial research model and hypotheses that have been constructed in phase three. Measurements in the questionnaire rely heavily on the available instruments designed in other related literature. Next, the sample size is defined, then the tentative questionnaire is pre-tested, also pilot study and questionnaire validity have been done before it is widely disseminated. The purpose of the pilot study is to consult the expertise in the relevant field in order to enhance content validity and to examine the reliability of the questionnaire prior to the actual survey. Once the validity and reliability of instruments are accepted, actual survey would be conducted on Palestinian's healthcare services. For pilot study and descriptive statistics, SPSS (version 18) software was used to produce the results. The output of this phase is the final research instrument and sample size.

3.2.5 Phase 5: Data Analysis

This phase involves the quantitative part of the study. The data analysis phase includes actual survey data collection, quantitative data analysis with SEM, model development and validation, and hypothesis testing. In this phase, the collected data was analysed by using SEM. Then, the relationships between constructs of security knowledge, attitude and behaviour were indicated and evaluated. In addition, nineteen hypotheses of the research were tested. The findings of the data analysis sessions help to identify security knowledge constructs that have a positive impact to behaviour. Furthermore, the findings of the research can be used to guide the organisations and professionals in cultivating and maintaining the security knowledge required to guide employee behaviour when interacting with information assets. The detailed discussion of this phase is contained in Chapter six, which achieves objective Three.

3.3 Research Design

Research design refers to a structured set of logical phases that maintains the progress of the study in the right track (Creswell, 2013). The researcher made use of a combined quantitative and qualitative approach for this research. The application of the above approaches is directly related to the objectives of the study (Creswell, 2013). According to Creswell (2013), the combination of both quantitative and qualitative methods in the research design gives strength to each of the two methods as well as decreasing their weaknesses. Hence, the quantitative research is used as a mean for testing objective theories via examining the relationship among variables. On the other hand, qualitative research is used as a mean for the exploration and understanding of the meaning that an individual or group of people attribute to a social or human problem. Usually, researchers of information system pay more attention to the use of either quantitative or qualitative approach, but the significance of combining these two research methods has started receiving more and more attention (Orozco, Tarhini & Tarhini, 2015). According to Creswell (2013) , the combination of research methods can be of great use for research areas in which certain phenomena are so complex that they require considering information from different perspectives.

To get an in-depth, this research will employ mixed methods research approach to collect data. The rationale for mixed methods research approaches is that the method provides a comprehensive and complete understanding of the results (Creswell, 2012,2013; Baskerville, Hogg & Lemelin, 2001).The purpose of a qualitative study through semi-structure interviews in this research is to gain an in-depth understanding of the security knowledge constructs to influence the employee behaviour in organisations. The results of the interview were used to identify security knowledge constructs, including its antecedents and outcomes which then lead to the modification of the research model. In addition, the findings from the interviews will assist in developing the items in the questionnaire for the next phase of quantitative data collection. The quantitative study through survey questionnaire in this research is to gain statistical results that help to identify the impact each of security knowledge constructs to behaviour.

This research applied an exploratory sequential design (Creswell, 2013). The rationale for this approach is that to explore the security knowledge constructs that required to influence the employee behaviour within organisations. The qualitative findings help to confirm and refine the security knowledge constructs in the research model, which is then used to develop the questionnaire to be used in the quantitative study. Figure 3.2 depicts the exploratory sequential design in this study. The semi-structured interview is used to obtain information from a group of information security expertise in the first phase. This is then followed by quantitative data collection from the employees in healthcare sector in the second phase. The results from the qualitative study in Phase 1 will be employed to provide a focused questionnaire for Phase 2 as depicted in Figure 3.2.

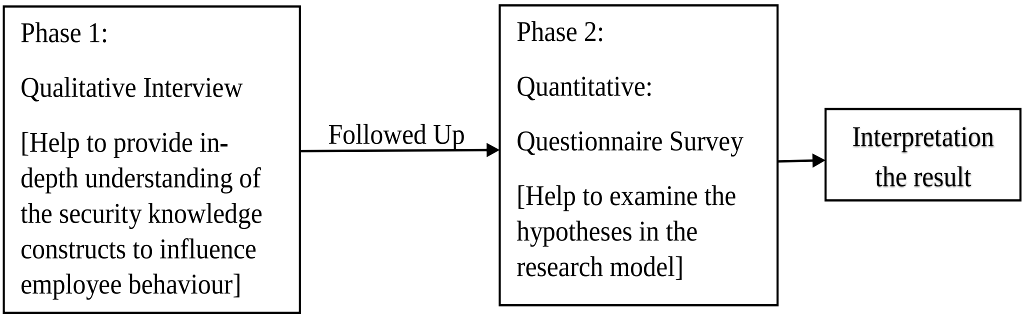

Phase 1:
Qualitative Interview
[Help to provide in-depth understanding of the security knowledge constructs to influence employee behaviour]
Followed Up
Phase 2:
Quantitative:
Questionnaire Survey
[Help to examine the hypotheses in the research model]
Interpretation the result

Figure 3.2 Depicts the exploratory sequential design in this study

3.4 Qualitative Data Collection

In this section, the qualitative data collection method and instrument are presented. According to Myers (1997), qualitative research methods are generally used by researchers to examine social and cultural phenomenon in the field of social sciences. He added that such methods assist researchers to have an in-depth view of individuals, social and cultural contexts wherein they reside. Similarly, Glaser & Strauss (2009) emphasized on the importance of the role of qualitative research in understanding people’s perceptions and actions, behaviours which cannot be understood only through observation or when people are questioned about them.

Creswell (2013) contended that interviews are the primary qualitative data collection technique and as such, the interview method was adopted in this study. In the case of information security culture, Zakaria (2004) has recommended the use of semi structured interviews to collect information regarding employees’ assumptions, real and implicit security behaviour in information security culture research. The interview method assists in obtaining, understanding and confirming the collected information. The interview method would also help to understand and confirm the security knowledge constructs collected through literature review.

The purpose of a qualitative study through semi-structure interviews in this research is to gain an in-depth understanding of the security knowledge constructs to improve the employee behaviour in organisations. Given below are the justifications for using the semi-structured interview:

- To explore the constructs of security knowledge by making sure that the six constructs create security knowledge required to influence employee behaviour in organisation.
- To gain an in-depth understanding of the security knowledge constructs to influence the employee behaviour in organisations.
- The findings from the interview will assist in developing the items of security knowledge construct.
- The interview method assists in obtaining, understanding, exploring and confirming the security knowledge constructs.
- To shed light on the contents of the constructs of security knowledge.
- To determine new issues/information on enhancing security knowledge required to influence employee behaviour that may not have been discussed before.
- To determine the training programs linked to security awareness in order to comprehend the security knowledge construct provided to employees.
- To confirm the results reported in literature of studies that identified security knowledge required for enhancing employee behaviour.
- To obtain rich information from the information security specialists who are directly involved in the information security in organisations.

3.4.1 Types of Interviews

There are three types of interviews namely, structured, semi-structured and unstructured. Their definitions are given below (Hogail, 2015).

- Structured interviews are interviews with definite questions and responses to obtain specific information.
- Semi-structured interviews are interviews with pre-defined questions are asked but open answers are expected providing freedom of expressing views and opinions.
- Unstructured interviews are interviews with neither specified questions nor answers but are open to explore the phenomenon during the interview for complete exploration of the issue under study.

With regards to the above types of interviews, in the discipline of information systems, semi-structured interviews are often used when:

- The researcher is in the earlier phases (Benbasat, Goldstein, & Mead, 1987; Gable, 1994).
- This type of interview is often used in information security culture studies that need development of theories to shed light and predict actual practices (Alnatheer, 2014). Hence, the present study adopts semi-structured interviews with open-ended questions for collecting qualitative data.
- Further, the main reasons for adopting semi-structured interviews are due to their advantages in gathering factual information, collecting statements regarding individuals' opinions and exploring in depth interviewees' experience, reasoning, and motivation (Drever, 2003).

The interviewees comprise of security experts who were chosen based on their multidisciplinary experience to eliminate potential bias that may be represented by one type of specialist. Hence, five experts have been selected to be interviewed; two from the academic field in information security, while the rest are information security specialists from various companies.

3.4.2 Interview Design

According to (Brenner, 2006), interview is the most appropriate method to collect views and experiences from a few participants. Oftentimes, interviews comprise of the delivery of open-ended questions to the interviewees and recording down and noting their replies (Creswell, 2013). He added that interviews provide valuable and useful information and they enable participants to freely describe their personal experiences and knowledge. It enables them to provide confidential information to enrich the phenomenon's description in a way that quantitative methods are unable to obtain.

Creswell (2013) further explained that interviews may be carried out in different ways such as face-to-face, email, telephone or in focus groups. This study made use of individual telephone and face-to-face interviews to obtain the required data from the interviewed experts. The researcher provided open-ended questions to the interviewees and gathered required data to answer the research questions. The interviews were aimed to explore the IT security experts' opinions and attitudes towards the security knowledge constructs that is significant to be imparted to employees for the enhancement of their behaviour. The interview guideline was developed by analysing data from prior literature concerning security knowledge. The open ended nature of the questions encourage the flexibility of the interviews and offer the chances of asking additional questions when appropriate. This can assist in gaining more in depth information from the participants.

3.4.3 Interview Data Collection Procedure

Creswell (2013) explained that qualitative data collection requires data to be collected from several individuals/sites. Also, Howe & Eisenhart (1990) revealed the data collection techniques in qualitative research should match the research questions to be completely answers. This method allows to answer the first question of this study in order to obtain answers.

In mixed methods research, the qualitative data collection usually employs purposive sampling which involves the selection of certain units or cases ''based on a specific purpose rather than randomly'' (Flick, 2009). In purposive sampling, possible participants are selected because they yield the most relevant information for the study on the basis of known characteristics (Flick, 2009). Such selection based on Creswell (2013) study, is largely dependent on people and places that provide the best information to the core phenomenon of the study. He also stated that the choice of participants hinges on the rich information they can provide and thus, interviews of information security specialists and academic experts were chosen for this study in order to understand the subject and obtain accurate knowledge from them.

In a related study, Jakobsen & Johansen (2004) conducted interviews to investigate the information culture in health information system. They interviewed information managers as the key people at regional and district levels. This implies that the step of choosing information managers for the interviews is a vital step in gathering data. In the same vein, Jakobsen & Johansen (2004) conducted his interviews with various representatives from professional information managers, academics, administrators and educational design staff.

Thus, key managers of information security are chosen for the interviews to provide the needed information regarding their organisation. In addition, academic experts were also interviewed from the field of information security to provide information from the academic perspective.

3.5 Population and Sampling Frame

Bryman & Bell (2015) defined population as the universe of objects, from which the sample is selected, and they defined a sample as the population segment that is chosen for examination. There are two types of sampling methods namely probability and non-probability sampling, with each having its own divisions and categories. The primary difference between the two is that in probability sampling, each object has equal opportunity of being chosen, while in the non-probability sampling, the chances that an object can be chosen are unknown (Bryman & Bell, 2015; Saunders, 2011).

There are various ways to determine the appropriate sampling size for conducting a survey questionnaire. Comrey & Lee (1992) claim that a sample size of 100 respondents is considered poor, 200 considered fair, 300 considered good, 500 considered very good, and 1,000 or more considered excellent. In another argument, Wimmer & Dominick (2006) assert that in multivariate studies, a large sample is required because of the inclusion of multiple response data analyses. The sample size of 250 respondents is recommended as good, 500 as very good, and 1000 as excellent.

In another take on the sample size, Watson (2001); Sekaran (2009) related that the determination of the suitable sample size involves taking three criteria into account and they are confidence level, precision level (sampling error) and variability. However, Watson (2001) recommends avoiding determining a sample size randomly, or affix a percentage to it, because there is no exact percentage for each population. In light of this, Krejcie & Morgan (1970); Sekaran (2005) perform an arithmetical equation to calculate the sample size, and this is reproduced as follows:

$$S=X^2*N*P(1-P) \div d^2 *(N-1)+ X^2*P*(1-P) \qquad \text{(Equation 3.1)}$$

(Krejcie & Morgan (1970); Sekaran (2005))

Where,

S = the sample size

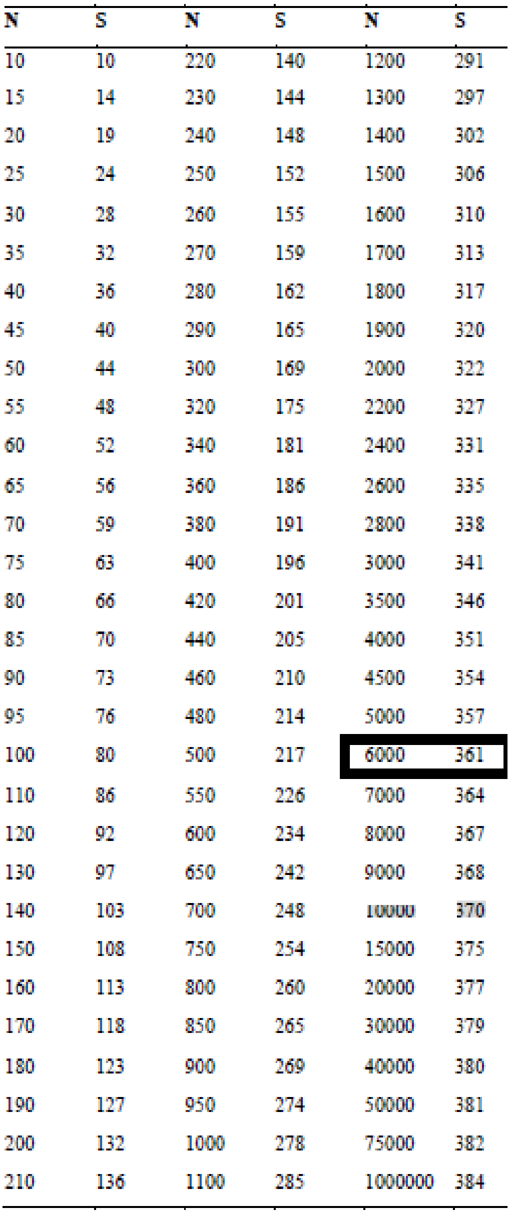
X^2 = the value of chi-square for 1 degree of freedom at the desired confidence level (3.841/95%)

N = the population size

P = population proportion (as known, variability)

d = the degree of precision level (known as sampling error or margin error)

As mentioned, for the calculation of the sample size and the mitigation of percentage of errors its calculation, prior studies (Krejcie & Morgan (1970); Sekaran (2005) ;Payne & McMorris (1967); Dattalo (2008)) set up a sample table that depicts the size of the sample on the basis of the size of the population based on the above equation. Therefore, in this study, the actual population is first established. There are 6000 employees working in the Palestinian Healthcare services with the exclusion of the employees working the service section, drivers and other healthcare employees that do not need computers for their tasks. This figure was provided by the Palestinian Health Information Centre (PHIC), (PHIC, 2016). Based on Figure 3.3, the sample size should be 361 (out of 6000 population) and therefore, this study use this sample size.



N	S	N	S	N	S
10	10	220	140	1200	291
15	14	230	144	1300	297
20	19	240	148	1400	302
25	24	250	152	1500	306
30	28	260	155	1600	310
35	32	270	159	1700	313
40	36	280	162	1800	317
45	40	290	165	1900	320
50	44	300	169	2000	322
55	48	320	175	2200	327
60	52	340	181	2400	331
65	56	360	186	2600	335
70	59	380	191	2800	338
75	63	400	196	3000	341
80	66	420	201	3500	346
85	70	440	205	4000	351
90	73	460	210	4500	354
95	76	480	214	5000	357
100	80	500	217	6000	361
110	86	550	226	7000	364
120	92	600	234	8000	367
130	97	650	242	9000	368
140	103	700	248	10000	370
150	108	750	254	15000	375
160	113	800	260	20000	377
170	118	850	265	30000	379
180	123	900	269	40000	380
190	127	950	274	50000	381
200	132	1000	278	75000	382
210	136	1100	285	1000000	384

Figure 3.3 Depicts the sample size from a given population size

3.6 Sampling Technique

In this study, the purposive sampling technique of data collection was adopted – this type of data collection is probability sampling method. It requires survey respondents to have distinct characteristics that are related to the aims of the exploratory survey (Dörnyei & Taguchi, 2009; Trochim, 2006). Along a similar line of claim, Sekaran (2005) related that purposive sampling is limited to specific types of group(s) that are capable of providing the required information either because the group is the one of the few that can provide such data, or it adheres to the criteria that the study is on track of. The type of sample used in this sampling technique may take the form of society, organisation or exclusive group (Trochim, 2006).

In this study, the use of purposive sampling entailed the collection of data from the healthcare service section specifically from employees who are using computers and laptops to perform their work.

3.7 Questionnaire Translation

The native language in Palestine is Arabic and as such, the original English version of the questionnaire was translated into Arabic (see Appendix A). Regardless of the translation, the respondents were requested to choose whether they want to fill the English or Arabic questionnaire, with majority of them eventually opting for the latter.

Accurate translation of the questionnaire had to be ensured for clarity and understanding, and thus, the two main translation procedures recommended by Adler(1983) were employed:

1) Back translation – involves the translation of the initial questionnaire into Arabic language, and back-translating it to English.

2) Expert translation – involves the translation of the questionnaire by an expert who is proficient in English and Arabic language and the topic under study.

Differences were noted between the two language versions of the questionnaire and therefore, the best version of the translated questionnaire was developed by focusing on the content and the context. The Arabic questionnaire version was tested using five participants in a pilot study and their feedback was obtained with respect to its clarity and the understanding of questions. Both translated copies were then sent to a translator employed by the "Kittani cultural centre for training, languages and translation in Palestine". Subsequently, a certificate of translation was obtained from the centre (see Appendix B).

3.8 Data Gathering by Questionnaire

Questionnaire is a research instrument consisting of a series of questions or prompts in order to gather information from respondents (Oates, 2006). It can be used for exploration, description, or explanation of a case study context (Pinsonneault & Kraemer, 1993). Questionnaire helps the researcher to become more familiar with a phenomenon of interest. Zakaria (2004) suggested the use of questionnaire for data collection on employee's perceptions of actual security behaviour in the field of information security culture.

Okere et al. (2012) stated that there is no method or a toolset to assess information security culture as there is no published or widely accepted and consolidated approach that provided how to assess the culture and more research in this area is needed. However, one way to measure the status of an organisation's information security culture is to use a questionnaire such as one proposed by Da Veiga, Martins & Eloff (2007) ; Schlienger & Teufel (2003) to achieve an understanding of factors that influence the employees security behaviour. Furthermore, Da Veiga et al. (2007) have validated an instrument for assessing the information security culture. The purpose of using questionnaire is to determine the influence of security knowledge constructs on employee behaviour. The following the reasons explain the using of questionnaire:

1. Help to identify the impact each of security knowledge constructs to behaviour.
2. To examine the research hypothesis in KAB model.
3. To confirm or reject the hypothesis in KAB model.
4. To examine the mediation effect between security knowledge constructs on behaviour.

Several advantages were listed by Da Veiga (2008) ; Da Veiga et al., (2007) from their use of questionnaire to assess information security culture, as stated below:

- Questionnaire is able to identify areas of concern and areas that require improvements with regard the information security culture.
- Questionnaire can help organisations to specify the current and the desired information security culture, and recognize the change of actions required to accomplish the desired information security culture.
- The information obtained from questionnaire can influence future management decisions such as more awareness, training or resources allocations.
- The questionnaire could be a way of raising awareness regarding information security. It also helps to increase the commitment of organisation's employees as they feel that they are part of the process.

The above objectives and advantages are aligned with those of the study in that the findings of the study are expected to assist the management to furnish the desired information culture by focusing on security knowledge required that must be inculcated between employees for the enhancement of their behaviour. It is pertinent for management to determine suitable techniques for the promotion of awareness and knowledge among employees.

Aside from the advantages of the questionnaire as highlighted above, questionnaire is easy to administer compared to other methods, it is cheap to administer compared to other methods, and standardized answers are provided to make it simple for compilation of data. However, standardized answers in questionnaires may lead to frustrations among respondents. A questionnaire is also confined by the fact that respondents need to be able to read the items and respond to them and sometimes, they find it difficult to interpret the items in a manner they were meant to convey. The construction and wording of the questionnaire also influence the collected data’s quality. More details on the questionnaire design and distribution are provided in the next sub-sections.

3.8.1 Questionnaire Design

The development of a research instrument in this study gathered measurements items and adopted them from prior studies, with modifications. The survey instrument comprises of quantitative items.

The researcher made sure that the questionnaire is complete by adopting a designed framework for questionnaire construction laid down by Churchill (2001) ; Gilbert Churchill, Brown & Suter (2004). Some modifications were made to suit the study objectives. Figure 3.4 displays the designed framework for the questionnaire involving ten phases.

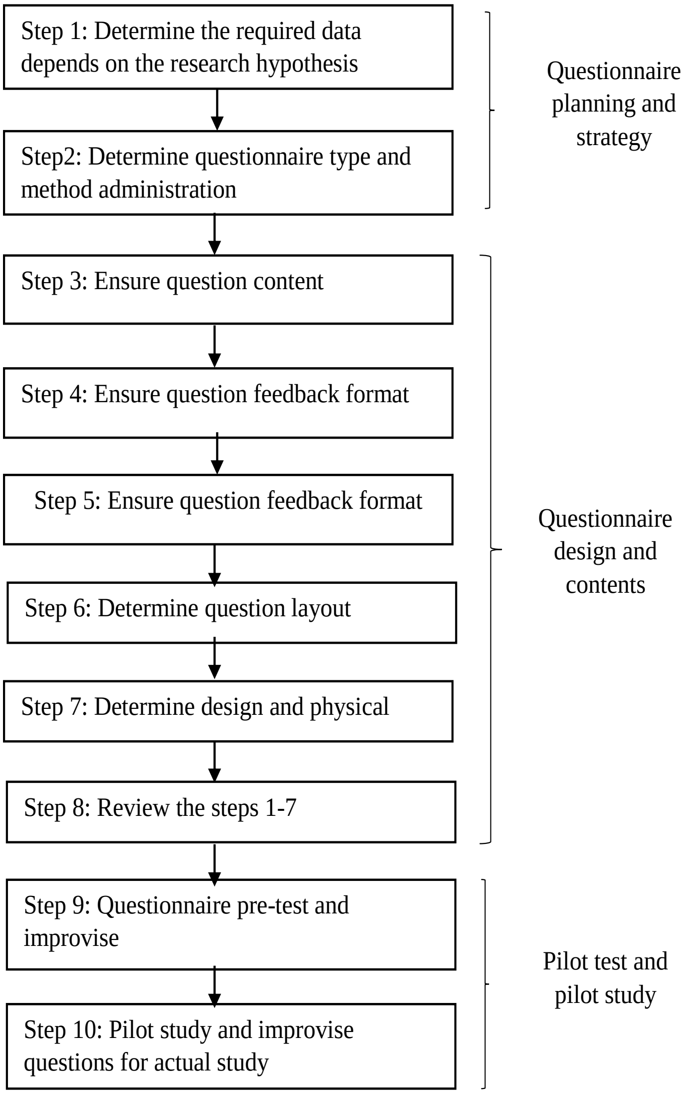

Step 1: Determine the required data depends on the research hypothesis
Step2: Determine questionnaire type and method administration
Step 3: Ensure question content
Step 4: Ensure question feedback format
Step 5: Ensure question feedback format
Step 6: Determine question layout
Step 7: Determine design and physical
Step 8: Review the steps 1-7
Step 9: Questionnaire pre-test and improvise
Step 10: Pilot study and improvise questions for actual study
Questionnaire planning and strategy
Questionnaire design and contents
Pilot test and pilot study

Figure 3.4 Framework for constructing the study questionnaire

a. Step 1: Determine the Required Data Depending on the Research Hypotheses

In this study, the researchers had to determine how to go about completing the development of the questionnaire at specified time and resources. Hence, prior to its construction, the objectives and hypotheses of the study were defined. The study hypotheses assist in determining the required data and its sources. This information lays down the relationship between the study constructs (Churchill, 2001; Sekaran & Bougie, 2009).

After data is gathered from the respondents, the hypotheses of the study are tested and analysed in order to achieve the research objectives. Prior studies (Raitoharju, Heiro, Kini, & D'Cruz (2009) and Straub, Loch & Hill (2003) discussed the challenges they faced during the data collection and analysis stage in difference the culture. It is therefore required to take the difference in culture into consideration in the questionnaire construction. In the context of this study, because the study was conducted in Palestine, the Arabic culture has been considered in formulation the questionnaire for the optimum outcome.

Step 2: Determining the Questionnaire Type and Method of Administration

Following the determination of what data to be collected, the type of questions to be presented in the questionnaire are determined, as well as the administration of the instrument. There are two types of questionnaires, namely, structured (close ended) and unstructured (open ended). In this study, the structured questionnaire is adopted for its easy to complete, and ensures that respondents are able to answer quickly and accurately. Furthermore, the nature of structured questionnaire helps to collect the kind of information that needed from respondent to answer the research question.

With regards to the administration of the questionnaire, it can either be personally administered or sent by mail (Sekaran ,2009). This study preferred personal administration of questionnaires based on several reasons, which are described below.

First, the questionnaire survey is confined to Palestine, and second, the general healthcare management was interested in the study and was inclined to provide their cooperation by requesting staff to fill in the questionnaire during working hours. The third reason is the survey questionnaire should be distributed to ensure the respondents and sections under target. Finally, the reason behind using personally administered questionnaires is the opportunity to encourage the completion of the questionnaires in a timely manner. This type of administration of questionnaire also provides a chance for the researcher to explain the importance of the study and to assist respondents in protecting their computers and their information assets.

Step 3: Ensuring the Questions Content (Survey Measurement Instrument)

The present study's latent variables are security knowledge constructs (knowledge of security threat, knowledge of organisation information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility and knowledge of security risk, behaviour and attitudes (see research model in Chapter Five for summary)).

a. Measurement Scale for Security Knowledge

This study employs the KAB (Knowledge, Attitude, and Behaviour) model for the presentation of the knowledge-behaviour relationship and it assumes that security knowledge constructs positively impact employee behaviour. The constructs are knowledge of security threat, knowledge of organisation information security strategy, knowledge of security knowledge, knowledge of legislation, regulation and national culture, knowledge of security responsibility and knowledge of security risk. Each security knowledge construct has a distinct influence on behaviour. The measurement items of the above mentioned constructs were adopted from prior related studies (refer to Tables 3.1 – 3.6).

Table 3.1 Measurement Scale for Knowledge of Security Threat

Knowledge of Security Threat	**References**
I know the types of harmful threats to information assets.	(Liang & Xue, 2009)
I know the negative consequences of an attack on or threat to information assets.	(Liang & Xue, 2009); (Ifinedo, 2011)

I understand that security threats (attacks) can occur any time.	(Liang & Xue, 2009);(Johnston & Warkentin,2012)
I know the threats and vulnerabilities towards the information assets in my work environment.	(OECD 2005); (Da Veiga & Eloff, 2010)
I know about information security threats.	Hall 1998

Table 3.2 Measurement Scale of Knowledge for Organisation Information Security Strategy

Knowledge of Organisation Information Security Strategy	**References**
I know what my organisation's information security strategy is.	(Von Solms & Von Solms, 2004; Da Veiga & Eloff 2010)
I know my organisation's information security strategy helps me protect my organisation's information assets in my daily work.	(Von Solms & Von Solms, 2004)
I understand the content of information security strategy elements like policy.	ISO/IEC 27001:2013
I know organisation's information security strategy helps me understand what is expected from me as an employee in terms of safeguarding my organisation's information assets.	(Von Solms & Von Solms, 2004; Da Veiga & Eloff 2010)
I know that my organisation has developed information security strategies to address the prevention and detection of threats and to respond to them.	ISO/IEC 27001:2013
I know information security requirements to protect information.	(ISO/IEC 27001: 2013)

I am aware of information security policies related to my job such as the password policy.	(Dojkovski et al. 2010)
I know that the information security is necessary to protect information in my organisation.	(Da Veiga & Eloff, 2010)
I know that the information security is necessary to increase the confidence that the third parties have in my organisation.	(Da Veiga & Eloff, 2010)
I know information security practices such as data encryption.	(Martins & Eloff, 2002)
I know information security practices such as a clear desk policy.	(Martins & Eloff, 2002)
I know about information security controls (e.g. that I must set up a strong password).	(Martins & Eloff, 2002)
I know the information security requirements helps me protect the information assets of my organisation.	(ISO/IEC 27001:2013)

Table 3.3 Measurement Scale for Knowledge of Security Technology

Knowledge of Security Technology	**References**
I know the technical tools and controls for information security helps me to preserve information security.	Alhogail,2015
I know the security technology enables me to help other employees with their technical queries and problems.	Alhogail,2015
I know that the appropriate use of technical controls is vital to achieve information security.	Alhogail,2015
I know the policy and guidelines for the effective use of information security hardware and software helps me preserve information security and prevent security breaches and threats.	Alhogail,2015
I know how to use technical measures such as antivirus to ensure information security.	(ISO/IEC 27001:2013)

Table 3.4 Measurement Scale for Knowledge of Legislation, Regulations and National Culture

Knowledge of Legislation, Regulations and National Culture	References
I know the government regulations regarding information security.	(Martins & Eloff, 2002)
I am aware of relevant government information security related legislation such as copyrights.	(Martins & Eloff, 2002)
I know the data protection and other relevant legislation and regulations.	ISO/IEC 27001:2013
I know the privacy and other relevant legislation and regulations.	ISO/IEC 27001:2013
I have clear directives on protecting sensitive and confidential information and applying the related regulations.	ISO/IEC 27001:2013
I am aware of the importance of the values of intellectual property and copy right laws.	ISO/IEC 27001:2013
I know the process of information security should not conflict with the society ethics and essential value.	(OECD 2005)
I know the national culture must be taken into account when designing information security policy and guidelines.	(OECD, 2005); (Alnatheer & Nelson, 2009)
I know the information security measures must comply with international standards.	(Martins & Eloff, 2002)

Table 3.5 Measurement Scale for Knowledge of Security Responsibility

Knowledge of Security Responsibility	References
I know that information security is my responsibility in the organisation.	(OECD, 2005)
I know that I am responsible for any actions that conflict with information security requirements.	(ISO/IEC 27001:2013)
I know what information security is.	(ISO/IEC 27001:2013)
I know how to report information security incidents.	(Da Veiga & Eloff, 2010)

I know my role with regards to each security policy.	(OECD 2005)
I know what to do when I detect a security violation.	(OECD 2005)
I know what information assets to protect and how I can protect them.	(OECD 2005)
I know that it is essential to protect information assets to achieve business success.	(ISO/IEC 27001: 2013); (Da Veiga, 2008)
I am aware that I should never give my password to somebody else.	(Jasber & Mustafa,2013; Rogers, 2002)

Table 3.6 Measurement Scale for Knowledge of Security Risk

Knowledge of Security Risk	**References**
I know that a weak password represents a security risk.	ISO/IEC 27001:2013
I know the risks when opening web links.	ISO/IEC 27001:2013
I know the security risks and dangerous to the information assets in my work environment.	Hall 1998
I know the risk when opening e-mails from unknown senders, especially if there is an attachment.	(Da Veiga,2008) (Martins & Eloff 2002)
I know the risk is when sharing passwords between others.	(Da Veiga, 2008)
I know the risk is when giving out confidential information of visit prohibited internet sites.	(Da Veiga, 2008)
I know it is essential to take care when talking about confidential information in public places.	(Martins & Eloff, 2002); (Da Veiga & Eloff, 2010)

b. Measurement Scale for Behaviour

Behaviour refers to a user's actual response to a recommended computer security behaviour (Ng, 2007). Security behaviour refers to an employee's ability to engage in appropriate and effective security actions (Blythe et al., 2015). Behaviour is the assumption about what behaviour regarding the protection of information is encouraged or not (Van Niekerk & Von Solms, 2010) .

In information security, the human factor comprises of two dimensions, which are knowledge and behaviour, and they are both interconnected (Van Niekerk & Von Solms, 2010). Employees have to be informed of the importance of information security so that they can protect the assets of the organisation. In this regard, they should understand and apply security knowledge and display suitable behaviour through such knowledge. There has to be alignment between knowledge and behaviour in order to influence employee behaviour in organisation. Table 3.7 lists the measurement items for behaviour adapted from prior studies in literature.

Table 3.7 Measurement Scale for Behaviour

Behaviour	**References**
I update the anti-virus software regularly.	ISO/IEC 27001:2013
I always lock my computer when I leave the desk.	ISO/IEC 17799:2013
I ensure that there is no confidential documents left on my desk when I leave the office.	ISO/IEC 17799:2013
When I suspect any information threat, I report it straightaway.	(Da Veiga & Eloff, 2010)
I should act in a way that prevents any threats to information security.	ISO/IEC 27001:2013
I share information about threats and vulnerabilities as appropriate.	(OECD, 2005)
I adhere to information security requirements in my organisation.	(OECD, 2005
I act in a supportive manner to prevent, detect and respond to security incidents.	(OECD, 2005)
I behave carefully when I connecting with email attachments especially from unknown senders.	Da Veiga,2008
I can easily ask question and leave comment regarded information security.	Alhogail,2015

I usually follow my organisations information security strategy in my daily work to protect information assets.	(Von Solms & Von Solms 2004); (Dojkovski et al. 2006; Da Veiga & Eloff 2010; OECD 2005)
I have a strong password.	(Martins & Eloff ,2002)
I do not open email attachments if the content of the email looks suspicious.	Alhogail,2015
Before reading an email, I will first check if the subject and the sender make sense.	(Jasber & Mustafa,2013); (Rogers, 2002)
I never give my personal information (like home/email address, telephone number, etc.) to unknown websites.	(Jasber & Mustafa,2013); (Rogers, 2002)

c. Measurement for Attitude

Attitude focuses on “what an employee think” (Kaur & Mustafa, 2013) . Providing the knowledge for the employee’s will lead to changes in their attitudes, views and knowledge. This will have a positive impact to the employees’ behaviour in organisation (Alhogail, 2015; Da Veiga & Eloff, 2010; Kaur & Mustafa, 2013). This study thus considers the importance of attitudes towards understanding the security knowledge constructs that contribute to enhancing the behaviour of employees.

Security knowledge should be inculcated to every employee to direct their attitude and behaviour, where attitude is considered to mediate the security knowledge-behaviour relationship. Table 3.8 contains the measurement items adapted from prior relevant studies.

Table 3.8 Measurement Scale for Attitude

Attitude	References
Knowing the types of security knowledge required in my organisation is necessary.	Safa & Von Solms, 2015
Knowing the types of security knowledge required in my organisation is beneficial.	

My Attitude towards understanding the types of security knowledge required will have a positive effect on mitigating the risk of security breaches.	
Knowing the types of security knowledge required in my organisation is a valuable.	
My Attitude towards understanding the types of security knowledge required will have a positive effect on safeguarding the organisation's information assets.	
My Attitude towards understanding the types of security knowledge required will have a positive effect on decreasing the risk of information security incidents.	
My Attitude towards understanding the types of security knowledge required will have a positive effect on my security behaviour in my organisations.	

Step 4: Ensuring Question Feedback Format

This section presents the format for the responses to the items in the questionnaire to obtain the required data. The questions posed require a “yes” or “no” answer and multiple choice answers ranging from 1-5 or 1-7 (Churchill, 2001).

With regards to expedient response and increased rate of return of questionnaires, a short questionnaire comprising 5 pages with 70 items within was recommended by Ikhsan (2005). Following this suggestion, this study prepared a 5 paged questionnaire within which 70 items were included in the form of close-ended questions to ensure simplified response and data processing (Bryman & Bell, 2015; Sekaran, 2016).

The security knowledge items required to enhance employee behaviour were developed and identified by following guidelines. A cover letter was attached to the questionnaire that explains the researcher and university information as well as the objectives of the study to boost respondents’ participation in the survey (see Appendix C). The questionnaire had different parts, with each part having its own set of questions, and instructions were provided on the way they should be answered to mitigate ambiguity. The researcher thanked the respondents for their time, cooperation and invaluable feedback and cooperation.

There are nine parts to the questionnaire, with questions about demographic information, security knowledge constructs, attitude and behaviour. The first section covered the demographic information, while the remaining eight addressed knowledge of security threat, knowledge of organisation information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility, knowledge of security risk, attitudes and behaviour. The respondents were requested to tick the relevant answer in front of each item, measured by a 5-point Likert scale. The scale range depicted the following; 1- strongly disagree, 2- disagree, 3- neutral, 4- agree and 5- strongly agree. Likert scale was employed for its easy management, easy answering of questions and high reliability (Bryman & Bell, 2015; Chua, 2009). A 5-point Likert scale was specifically selected as it mitigates the possibility of measurement error and breach of normality in data distribution – in this regard, the Likert scale is a better option against other scales (e.g., Thurstone/Guttman).

As for the detailed contents of the sections; the first one contains the demographic details of the participants, requesting their age, year of experience, job level, education level, gender, work in IT department, education background, work requirements, and security awareness.

This is followed by the second section that contains items related to security knowledge required to enhance employee behaviour and this covers knowledge of security threat, knowledge of organisational information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility and knowledge of security risk. The third section contains behaviour, with the attitude construct covered in several questions.

Step 5: Determination of Appropriate Sentences and Clauses for Questions

The statements in the questionnaire should be appropriate, simple, clear and accurate as poor wording may lead to misunderstandings and incorrect answers (Churchill, 2001). The items should also be free of jargon and technical expressions that are unfamiliar to the respondents. Items that have been adopted and customized and validated in prior questionnaires may be adopted (Ismail & Yusof, 2009). It is important to steer clear of words that have double meanings, that are emotional in nature, and that go against the context culture (Oppenheim, 2000).

In the context of this study, Chua (2009) recommendations were followed to improve the quality of answers by making sure that the language is understandable, the words with double meanings are replaced, and the general knowledge and sensitive words are excluded.

Step 6: Determination of Questions Layout

This study followed the guidelines suggested by Chua (2009); Churchill (2001) ; Sekaran (2005) in determining the layout for the questions. These guidelines are:

- The initial question should be easy and attractive.
- The funnel approach be applied whereby questions range from general to specific.
- A heading be included for each part and set of questions.

The questionnaire opened with questions associated with demographic information, followed by sensitive questions (e.g. questions to test the hypotheses). Questions were also categorized according to the constructs they represent, and these constructs were grouped based on specific measurement values (e.g. security knowledge, attitudes and behaviour constructs), as suggested by (Chua, 2009).

Step 7: Determination of Design and Physical Shape of the Questions

It is important to professionally design the questionnaire to make sure that its clarity and credibility are established (Churchill, 2001; Sekaran, 2016). Items/questions that are well-developed produce higher rates of return and accurate answers (Balnaves & Caputi, 2001). The questionnaire should also provide the respondents with a clear direction to each dimension.

Step 8: Reviewing Steps 1-7 and Improvising

In questionnaire development, the contents and context have to be re-examined and revised. Therefore, steps 1-7 are revised to make sure that the layout of the items meets the measurement requirements of the study (Churchill, 2001). Therefore, the researcher made minor adjustments after revising steps 1-7 based on the guidelines established in prior studies.

Step 9: Questionnaire Pre-testing and Improvisation

Pre-testing of the questionnaire is crucial as all defects need to be identified and rectified before the actual survey is conducted (Sekaran, 2016). As proposed by Chua (2009) & Sekaran (2009), any questionnaire should be structured, tested, repaired, and tested again.

According to Chua (2009), the main purpose of pre-testing is to reduce bias and uncertainty, as well as to provide and maintain a high level of quality, reliability, and validity. A dependable validity of instrument scores ensures a meaningful translation of data (Creswell, 2013). Validity is defined as "an evaluation of the adequacy and appropriateness of the uses of assessment results" (Singh, Chan & Sidhu, 2006). A face validity test was performed by a team of experts to check and verify the capability of the instrument to measure what it is supposed to measure. Han (2010) indicates that either a formal or informal face validity test is necessary before instruments are applied for actual study. As all the measurement items for this study are adapted from previous studies, their validity has already been tested. However, due to possible differences in the scope and environment of the study, a formal face validity test was conducted by 10 experts in the area of this study, culminating in the adjustment and modification of the questionnaire. The aim of performing pre-test with experts is to see whether they understand the questionnaire statements and to evaluate the questionnaire in terms of its grammar, understanding, and clarity. The ambiguousness of the sentence can result in incomplete questionnaire by the respondents.

Supplementing the face validity technique, an expert panel was employed to refine the questionnaire. Ten experts that consist of academic researchers and specialist in IT security were consulted and their comments were taken into consideration to improve the design and effectiveness of the instrument. Several amendments were made to the questionnaire in order to exclude wrong vocabulary and grammar, typographical errors, duplicated meanings, long sentences, and words that respondents may have difficulty comprehending.

Step 10: Pilot Test and Final Validation of Questionnaire

Prior to the actual survey, a pilot study was conducted, which is a small-scale version of the actual one (Chua, 2009). In this study, pilot study was conducted to minimize bias in instrument text and format (Oppenheim, 2000; Sekaran, 2016).

The pilot study enabled the respondents to provide their feedback on the instrument in light of its format, content and terminology used. It also confirmed whether or not the respondents understood the items within and if they can complete it in a reasonable time. Based on the feedback, the respondents took 16 minutes to complete the questionnaire, and this falls within the time frame (10-20 minutes) recommended by Chua (2009).

Moreover, a pilot study has its advantages as discussed by (Creswell, 2013). It minimizes ambiguity, highlights difficulties in interpretation and understanding of items, and pinpoints items that are confusing and biased. He added that a pilot study is a procedure where the research is provided an opportunity to rectify the errors in the instruments on the basis of small number individuals' feedback on it. This guarantees that the individuals are capable of completing the survey in an accurate and timely manner.

Therefore, this study conducted a pilot test to validate the instrument before administering the actual survey. According to Cooper, Schindler & Sun (2003), an approximate sample size for pilot study should be between 25 and 100. Based on this, a total of 30 respondents have been selected for the pilot study. They were selected by convenience sampling from different healthcare and were requested to fill in the questionnaires and leave their feedback, which was used to refine the instrument, ensuring its effectiveness in data collection. Lodico, Spaulding, & Voegtle (2010) stated that a pilot study saves survey studies from failure through the respondents' identification of complicated, confusing and offensive items.

A pilot study was conducted to examine consistency of the questions and the respondents understanding level to the questionnaire. Moreover, pilot study has saved so many survey studies from failure by using suggestion of the respondents to identify and modifying complicated, confusing or offensive questions'. Convenience sampling was employed in selecting the sample in the pilot study. Convenience sampling is a sampling method that relies on data collection from population members who are conveniently available to participate in study.

In pilot study, both validity and reliability were tested again. Validity is defined as the accuracy of the instrument utilised in obtaining the data while reliability is defined as with consistency of data. Lodico et al. (2010) expressed the view that correlational studies should show proof of the validity of the instruments used and reliability of the data collated, and suggested the use of a pilot study on a small sample of interested respondents in survey. Conducting a pilot test enables the researcher not only in determining the validity of the instrument used reliability of the data collated, but also in estimating the time required to implement the instrument (Slater, 1995). Table 3.9 contains the validity of items in the questionnaire confirmed by 5 of security experts.

Table 3.9 Calculating Validity of the Questions according to 5 Experts' Answers

Construct	**Item**	**Totally Suitable (5)**	**Suitable (4)**	**Moderate (3)**	**Unsuitable (2)**	**Totally Unsuitable (1)**	**Validity %**
Knowledge of Security Threat (KSTH)	KSTH1	3	1	1			88%
	KSTH2	3	1	1			88%
	KSTH3	4	1				96%
	KSTH4	3	2				92%
	KSTH5	4	1				96%
Knowledge of Organisation Information Security Strategy (KOISS)	KOISS1	3	1	1			88%
	KOISS2	2	2		1		80%
	KOISS3	3	2				92%
	KOISS4	4	1				96%
	KOISS5	3	2				92%
	KOISS6	3	1	1			88%
	KOISS7	3	2				92%
	KOISS8	2	2	1			84%
	KOISS9	2	3				88%
	KOISS10	4	1				96%
	KOISS11	4	1				96%
	KOISS12	3	1	1			88%
	KOISS13	4			1		88%
Knowledge of Security	KSTG1	3	2				92%
	KSTG2	3	2				92%
	KSTG3	3	1	1			88%

Technology (KSTG)	KSTG4	3	1	1		88%
	KSTG5	2	2	1		84%
Knowledge of Legislation, Regulation and National Culture (KLRNC)	KLRNC1	3	2			92%
	KLRNC2	4	1			96%
	KLRNC3	2	2	1		84%
	KLRNC4	2	3			88%
	KLRNC5	4	1			96%
	KLRNC6	4	1			96%
	KLRNC7	3	2			92%
	KLRNC8	4	1			96%
	KLRNC9	2	1	1		68%
Knowledge of Security Responsibility (KSRS)	KSRS1	2	2		1	80%
	KSRS2	3	1	1		88%
	KSRS3	2	1	1		68%
	KSRS4	4	1			96%
	KSRS5	5	0			100%
	KSRS6	3	1	1		88%
	KSRS7	2	2		1	80%
	KSRS8	2	1	2		80%
	KSRS9	3	2			92%
Knowledge of Security Risk (KSRK)	KSRK1	3	1	1		88%
	KSRK2	4			1	88%
	KSRK3	3	2			92%
	KSRK4	3	2			92%
	KSRK5	3	1	1		88%
	KSRK6	3	1	1		88%
	KSRK7	2	2	1		84%
Behaviour (BH)	BH1	3	2			92%
	BH2	4	1			96%
	BH3	2	2	1		84%
	BH4	2	3			88%
	BH5	4	1			96%
	BH6	4	1			96%
	BH7	3	2			92%
	BH8	4	1			96%
	BH9	3	2			92%
	BH10	4	1			96%
	BH11	3	2			92%
	BH12	3	1	1		88%
	BH13	3	1	1		88%
	BH14	4			1	88%
	BH15	3	2			92%
Attitudes (AT)	AT1	3	2			92%
	AT2	3	1	1		88%
	AT3	3	1	1		88%

	AT4	2	2	1			84%
	AT5	4	1				96%
	AT6	2	2	1			84%
	AT7	2	3				88%
						Total	**90%**

Table 3.9 lists the validity of the questionnaire from the consensus of 5 security experts. The total result of validity is 90%, which indicates a satisfactory result. After the experts' comments regarding the survey instrument's validity, 30 respondents were solicited for the pilot study to conduct proper statistical testing procedures for collected data reliability. The respondents were informed of the research purpose and the researcher answers the inquiries of respondents that aim to ensure that they were familiar with the contents of the research. The reliability of data and measurements were obtained through the use of Cronbach's alpha coefficient. Reliability has to be initially measured when assessing the instruments' quality (Churchill , 1979), and in this study, the general accepted values of Cronbach's alpha range from 0.60 to 0.70 as established by Hair et al. (1998).

The results of the reliability tests from 30 respondents' feedback in the pilot study are summarized in Table 3.10.

Table 3.10 Results of Reliability Test from Pilot Study

1st Order Constructs	**Item Number (70)**	**Internal Reliability**
Knowledge of Security Threat (KSTH)	5	0.855
Knowledge of Organisation Information Security Strategy (KOISS)	13	0.919
Knowledge of Security Technology (KSTG)	5	0.893
Knowledge of Legislation, Regulation and National Culture (KLRNC)	9	0.845
Knowledge of Security Responsibility (KSRS)	9	0.913
Knowledge of Security Risk (KSRK)	7	0.844
Behaviour (BH)	15	0.901
Attitudes (AT)	7	0.909

From the table, it is evident that the reliability of the constructs differed from 0.844 to 0.919 and they all exceeded the cut-off value of 0.70 (Hair et al., 2006). Evidently, the results met the required Cronbach's alpha (0.70 and over) and thus, reliability was confirmed (Hair, Black, Babin & Anderson, 2010; Sekaran, 2016).

Chapter Six contains detailed information on the reliability test involving confirmatory factor analysis (CFA) for convergent and discriminant validity. Such analysis was not suitable for the pilot study results owing to the minimal sample size, necessitating the assessment and examination of factors loadings to be performed following the collection of final data. The Cronbach's alpha was also obtained again on the final data.

3.9 Quantitative Data Collection

Self-administration of questionnaires was adopted in this study for data collection. Large samples of the population were distributed the questionnaire in order to collect data by the respondents in healthcare services. The distribution and retrieval of questionnaires took place from January 2017 to May 2017. This type of questionnaire has been known to provide high response rate.

3.9.1 Final Study

The questionnaire was distributed to Palestinian healthcare services with the total number of distributed questionnaires being 400. From the total number, 390 were retrieved, and only 361 were found to be suitable for data analysis.

3.9.2 Data Analysis

The research objectives and hypotheses provided a foundation to determine the most appropriate methods to analyse the data collected from the surveys. The data collected from the survey were analysed by Analysis of Moment Structures (AMOS) version 20 as well as Statistical Package for Social Sciences (SPSS) version 18.

The AMOS was selected as covariance based Structural Equation Modelling (SEM) software due to the presence of adequate theoretical information and no complexity in the model. That is, the appropriate variables are chosen and linked together in the process of converting a theory into a structural equation model (Blunch, 2012). Furthermore, since the proposed model in this study was developed upon the established theories with minor changes, AMOS was used to confirm or reject the theories through testing of hypothesis (Chin & Newsted, 1999) .

This study used AMOS for the analysis of convergent validity and discriminant validity through confirmatory factor analysis (CFA) to assess the adequacy of the measurement model (stage 1). In conducting path analysis, the AMOS software was used again to examine the research hypotheses and construct the structural model (stage 2). The SPSS was used to detect univariate outliers and conduct the frequency analysis (i.e., sample profile), descriptive analysis and internal reliability or Cronbach Alpha.

3.10 An Overview on Structural Equation Modelling (SEM)

Structural Equation Modelling (SEM) analysis comprises of two major stages, the measurement model or confirmatory factor analysis (CFA) and the structural equation model. The measurement model (CFA model) is used to find out the links between manifest or observed and latent or unobserved variables. The measurement model could therefore be said to define the manner in which latent or unobserved variables are assessed in terms of the manifest variables (Ho, 2006). As suggested by Hair et al. (2006), individual CFA was performed for each of the constructs followed by the measurement model of study which provided specifics and evaluation based on the Goodness-Of-Fit (GOF) indices and evidence of construct validity. This study employed the Maximum likelihood Estimation (MLE) as the extraction technique. This is one of the most widely used estimation methods that allow testing of individual direct effects and error term correlation.

As mentioned earlier, one of the main advantages of the SEM is its ability to assess construct validity of measurements. In this instance, construct validity refers to the accuracy of measurements (Hair et al., 2006). In SEM analysis, construct validity is assessed by two main components which are convergence validity and discriminant validity. Convergent validity refers to the similarity in degree of variance between the items which are the indicators of a specific construct. The convergent validity could be measured by considering the size of factor loading (standardized regression weights), Average Variance Extracted (AVE), and Composite Reliability (CR) among sets of items in the construct. The factor loading estimates with values 0.5 or greater and extracted average variance of 0.5 or higher show adequate convergence among the items in the construct (Hair et al., 2006). The average variance extracted can be calculated by dividing the sum square of the standardized factor loading by the factor loading number. The composite reliability (CR) should be 0.6 or higher to show adequate internal consistency (Bargozzi & Yi, 1988). The CR is computed from the square sum of factor loading and sum of error variance terms for a construct (Hair et al., 2006).

Discriminant validity refers to the issue of how truly distinct a construct is from other constructs. Discriminant validity can be assessed by comparing the square root of the AVE for two constructs and their correlations. Evidence of discriminant validity is when the correlation between the two constructs is smaller than the square root of the AVE for each construct (Fornell & Larcker, 1981; Hair et al., 2006). Furthermore, correlations between the factors should not exceed 0.85 (Kline, 2005).

The measurement items that represent each individual variable should also be verified through internal reliability analysis. Reliability is the degree to which a measure is error-free. To ensure that the items produce a reliable scale, Cronbach's alpha coefficient of internal consistency should be examined. The higher value of Cronbach's alpha refers to higher reliability, with a range from 0 to 1. Nunnally and Bernstein suggest that for a reliable scale, Cronbach's alpha should not be lower than 0.7 (Nunnally & Bernstein, 1994).

The main assumption in using MLE is the normal distribution of the data. As a general rule of thumb, the data may be assumed to be normally distributed if skew and kurtosis is within the range of -1 to +1, or -2 to +2 or even 3 (Lomax & Schumacker, 2012). Byrne (2013) suggested using a cut-off point of less than 7 as an acceptable value for the kurtosis. She added that the data which is skewed within the range of -3 to +3 could be considered as being normally distributed.

The SEM is distinguished by the ability of its overall model fit and its ability to assess the construct validity of a proposed measurement theory in addition to being the tool required to check reliability (Hair et al., 2006; Ho, 2006). A number of Goodness-Of-Fit (GOF) indices exist for the assessment of the overall fit of individual construct CFA, measurements of overall CFA and hypothesized structural models. The Goodness-Of-Fit

(GOF) indices provide the factors to investigate the level of coincidences in the covariance matrix of the proposed model against the sample covariance matrix (Kline, 2005). In general, there are three categories of Goodness-of-Fit indices, namely:

A. Absolute fit measures such as Chi-square statistic, Goodness-Of-Fit statistic (GFI), and Root Mean Square Error of Approximation (RMSEA).
B. Incremental fit measures such as Tucker-Lewis Index (TLI), Normed Fit Index (NFI), Incremental Fit Index (IFI), and Comparative Fit Index (CFI).
C. Parsimonious fit measures such as Akaik Information Criterion (AIC) and Parsimonious Normed Fit Index (PNFI).

The Chi-square ($\chi 2$) statistic, generally considered as one of the most important absolute fit indexes, is the tool for researchers seeking a non-significant value in support of their proposed model being able to significantly reproduce the sample covariance matrix. However, when the sample size increases, the $\chi 2$ statistic shows a significant p-value (Lomax & Schumacker, 2012). When the $\chi 2$ model fit index shows a significant p-value it does not mean that the proposed model cannot be interpreted or that it is completely unacceptable. The researcher can resort to using the other GOF indices. Goodness-of-Fit Index (GFI) is a non-statistical index ranging from 0 (poor fit) to 1 (perfect fit) (Ho, 2006). GFI values of over 0.90 indicate a good fit (Hoyle, 1995). Root Mean Square Error of Approximation (RMSEA) is another absolute fit index which should be lower than 0.1 to indicate a good fit (Schumacker and Lomax, 2010). However the RMSEA values of between 0.03 and 0.08 show a better fit model (Hair et al., 2006; Ho, 2006). For incremental fit indices such as TLI, NFI, IFI, and CFI, values range between 0 (poor fit) to 1 (perfect fit). The values of 0.90 and above show that there is a good fit between the model and the data (Bargozzi & Yi, 1988; Hair et al., 2006; Ho, 2006). Akaik Information Criterion (AIC) and the Parsimonious Normed Fit Index (PNFI) is normally used where comparison of the models with lower AIC values (near to 0) and higher value PNFI indicates a better fit and better parsimony (Ho, 2006). Hair et al. (2006) proposed the use of three to four fit indices for adequate evidence of model fit. These should ideally include one incremental index, one absolute fit measure and the Chi-square value and associated degrees of freedom. Therefore, in this study, absolute fit measures such as Chi-square statistic, Relative Chi-square ($\chi 2$/df), GFI, AGFI and RMSEA were used and among the incremental fit indices

TLI, IFI, and CFI were used to measure the level of model fit.

3.10.1 Justification for Using SEM

The AMOS was selected as Covariance Based Structural Equation Modelling (CB-SEM) to be used in this study to analyse the research model for several reasons including the size of the sample, the model complexity and the number of manifest as well as latent variables. The reasons are listed as follows:

1. The AMOS was selected as covariance based Structural Equation Modelling (CB-SEM) software due to presence of adequate theoretical information and no complexity in the model. That is, the appropriate variables are chosen and linked together in the process of converting a theory into a structural equation model (Blunch, 2012).
2. Since the proposed model in this study was developed upon the established theories with minor changes, AMOS was used to confirm or reject the theories through testing of hypothesis (Chin & Newsted, 1999) .
3. In this study we, combined some well-known theoretical models developed by the previous researcher and create some new relationships between the constructs. But the main body of the theoretical model is inspired from the literature. So it can be stated that the nature of this study is mainly confirmatory, therefore, AMOS was used to confirm the previous proposed models in the literature review.
4. SEM is suitable to use for sample size of more than 150 respondents. Therefore in this study the SEM is most suitable since the sample size is 361.
5. Past literature like Ringle et al. (2015) & Hair Jr et al. (2016) emphasized the appropriate use of PLS in exploratory studies. This study extends the KAB Model with minor changes and the nature of study is confirmatory and thus, SEM analysis is the most appropriate to be used.
6. PLS is suitable when the data is not normally distributed. In this study the data is normally distributes, thus SEM analysis is most appropriated to be used.

3.11 Conclusion

In this chapter, the study's research method was presented including the research operational framework, research design, target population, sample determination, measurement instruments and data collection methods. The chapter also contains a detailed explanation and discussion of quantitative data collection, its administration and the selected location of administration. The data processed to explicate quantitative data analysis through descriptive analysis, SEM and AMOS. An overview on structure equation modelling is presented in this chapter. Finally, a justification for using SEM also presented.

CHAPTER 4

QUALITATIVE ANALYSIS AND FINDINGS

4.1 Introduction

This chapter covers the qualitative analysis and findings. Section 4.2 presents the profile of the interviewees involved in this qualitative study. Section 4.3 presents the pilot study conducted before the actual interview. Then the interview validity and the interview process are covered in section 4.4 and 4.5 respectively. This is followed by section 4.6 that contains interview data analysis process. Section 4.7 presents the interview findings and discussing. Finally, section 4.8 summarizes the chapter and its contents

4.2 Interviewees Profile

The experts who were interviewed in this study were selected from multiple backgrounds. Such selection is aimed at eliminating any potential bias that might exist in one specialist. In general, the interviewees consist of information security practitioners working in the industry, and professors in the area of information security.

The interviewees were selected based on their role at the organisation in which they are working. To be qualified for this study, they should be responsible for information security and have been nominated by the contact person at each organisation. Interviews with Five information security experts were selected for the interview. Three of them are information security practitioners working in organisations, and they come from various positions (technical security expert, head of information and network security, and director of information security). They were chosen to be interviewed due to their experience in information security from the perspective of both technology and business. The remaining two interviewees are professors of information security working in an academic institution. They were interviewed either through face-to-face conversation or through phone conversation. The profiles of the interviewees are presented in Table 4.1.

Table 4.1 Interviewees profile

Interviewee	Position	Experience (year)	Duration (minutes)
1.	Technical Security Expert	10	50
2.	Head of Information and Network Security Department	12	40
3.	Director of Information Security	7	60
4.	Associate Professor- Information Security Track	10	70
5.	Associate Professor- Information Security and Networking Track	14	90

4.3 Interview Pilot Study

A pilot study was conducted using the designed semi-structured interview to ensure that the required information can be obtained from the interview. McBurney & White (2009) defined a pilot study as a "tentative, small scale study done by pre-test and modify study design and procedures". This is needed to check the accuracy and validity of the questions before the actual interviews. It will help to ensure appropriate wordings are used in the interview questions and to avoid any serious ambiguity. The pilot study is also used to check whether the interviewees' responses meet the purpose of the questions.

Three test interviews with information security professionals have been conducted. The pilot test aims at checking that there are no repeated questions, and questions are clear and not influencing the response of the participant. Moreover, the pilot test ensures that the interview measure what it aims to assess and can contribute to answer the research question.

Based on the comments and suggestions received from the pilot test, interview's questions were modified before using it is used in the actual interview in order to achieve better results. Few questions have been removed to eliminate a redundancy and some questions have been modified to improve the clarity of the questions.

4.4 Interview Validity

In order to construct interview's validity, some actions are taken. Firstly, having several data sources of evidence to ensure that bias is avoided (Creswell, 2002; Yin, 2003). This was done through identifying the security knowledge constructs from literature review, using interviews and questionnaire to collect the data. In addition, multiple individuals have been interviewed from different levels in information security.

Following each interview, this was sending the transcripts of the interviews to the interviewees by email for the purpose of verifying and checking descriptions. This led to discovering and correcting some minor descriptions.

Further, the findings obtained from the analysis of the interviews were also discussed with academic professor in the field of information security in both Arabic and English. This was to ensure that the translation was fully comprehensible.

4.5 Interview Process

Five semi-structured interviews with information security specialists were carried out through field visits or phone conversation during business hours. The interviews are scheduled in advance based on interviewees' availability.

Interviewees were selected based on their role at the organisation. They should be responsible for information security and have been nominated by the contact person at each case study. For ethical reasons, the identity of the interviewees and the data they provide are kept confidential, and the collected data is used for research only. The potential benefits of the interviews had been explained to participants before the interview started, in addition to their rights.

The interview was initiated by explaining the research purpose and assuring the respondents of the confidentiality of the information provided by them. The respondents were also provided with a description of the privacy arrangements and were given the freedom to participate or drop out at any time. They were not given any incentive for their participation in this study. The interview questions were delivered to the respondents via email prior to the interview sessions or directly by hand. Then, they were interviewed via phone or face to face interview that lasted between 40 and 90 minutes for each individual participant. Following this was sending the transcripts of the interviews to the interviewees by email for the purpose of verifying and checking descriptions. This led to discovering and correcting some minor descriptions.

The interviews process follows the following steps:

1. Establish contact with interviewee

2. Schedule the interview

3. Conduct the interview.

4. Transcribe the interview.

5. Provide access of the interview transcripts and study's findings to the participants.

The interviews are conducted in English and Arabic based of interviewee’s preference. However, all the transcripts are written in English. Only if the participant allowed recording, a voice recording machine is used. Otherwise, hand written notes are taken. Unfortunately, because of the sensitive nature of information security, some interviewees declined to have the interview recorded.

4.6 Interview Data Analysis Process

A qualitative analysis of the interviewee responses to the interview questions were conducted. The Interviewee’s responses were scripted for content analysis and review. The data analysis is based on the data amount in that data of less than 500 pages are analysed by hand as recommended by (Creswell, 2013). In this study, due to the small qualitative data obtained, data analysis was manually conducted.

After the semi-structured interviews, data analysis was carried out. The analysis involved four phases namely transcribing, organizing, coding, and themes building (Creswell, 2012). Firstly, audio recorded data and handwritten notes gained from the interviews were transcribed to word processor text. Transcripts of interviews were then presented to the respondents for validation purposes to ensure that the interview had captured the intended meaning of the respondents. Then, the interview transcripts will be organized into sections for easy retrieval in the organizing phase. Subsequently, the transcribe interviews were coded. In the coding phase, the transcripts were read repeatedly to highlight parts of the text and to emphasis the sections and issues that seemed to be important and relevant.

The interviews transcripts were divided into two segments were identified to summarize the data (Creswell, 2013):

1. Segments that seem to have no relation to the research, which were subsequently ignored.

2. Segments that appear to be relevant to the research question.

Then, the focus is drawn to the second segment, or unit of data (words, phrases or paragraphs that are relative to the research question).

Finally, similar codes were grouped together as a theme or category to form a major idea in the themes building phase. The coded data were reviewed to identify areas of similarity and overlap between codes. Codes that seem to share some unifying feature were clustered into a themes.

In summary, the interview analysis involved the following steps:

1. Transcript the interview.
2. Organize, identify code and themes (category) for the analysis of the interview transcripts.
3. Combine response to each question in one single document.
4. Draw the conclusion.

The analysis strategy is portrayed in Figure 4.1.

Organizes in the data were identified, which were selected in order to answer the research question. This helps to reduce amount of data into a small number of analytic units which is used to categorize the security knowledge constructs. The analysis involves taking one piece of data and comparing it with all the others that may be similar or different in order to develop possible relations between various pieces of data (Creswell, 2013). The main categories are knowledge of security threat, knowledge of organisation information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture related to security filed, knowledge of security responsibility and knowledge of security risk.

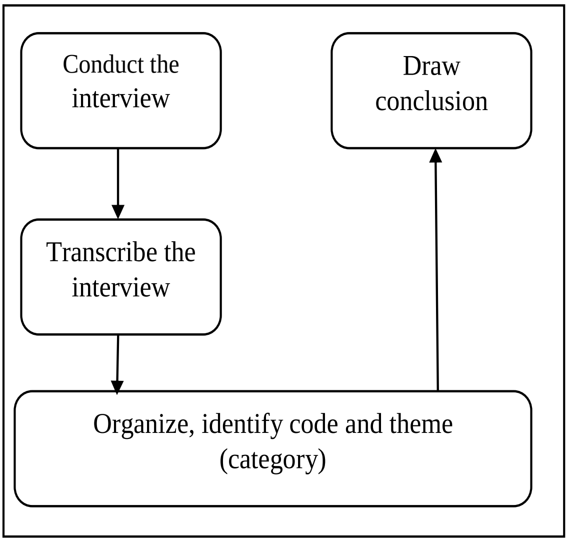


Figure 4.1 Interview analysis process

4.7 Discussion and Findings

Triangulation between the findings of literature review and the findings of semi-structured interview regarding identifying the security knowledge constructs to influence the employee behaviour in order to answer the first research question has been considered in this research. The aim of triangulation is to test the consistency of findings obtained through different instruments. Triangulation is defined as the mixing of data methods so that diverse viewpoints or standpoints cast light upon a topic (Domanski, 2004). The mixing of data types, known as data triangulation means using more than one method to collect data on the same topic. This is a way of assuring the validity of research through the use of a variety of methods to collect data on the same topic (Domanski, 2004). In this research, in order to answer the first question, a literature review has been conducted to focus on the studies that identified or discussed the relation between knowledge and behaviour that help to identify the security knowledge needed to influence the employee behaviour within organisation (section 2.8). The finding of literature review is to identify the security knowledge construct to influence employee behaviour. After that, a semi-structured interview has been conducted with a group of information security expertise to identify the security knowledge needed to influence the employee behaviour based on their expertise. The aim of semi-structured is to ensure all of these security knowledge constructs are relevant to help influence the employee behaviour in organisations, to explore and to gain an in depth understanding of security knowledge constructs that are required to influence the employee behaviour in organisations. It also aims to obtain their opinions and feedbacks concerning knowledge needed to influence employee behaviour in order to explore the variables and principles of security knowledge. The findings obtained from the interviews that all the interviewees confirmed that the security knowledge constructs are all relevant to help influence the employee behaviour in organisations. Semi-structured interview has been followed after conducting the literature review to ensure there is consistency between the findings of literature review and the findings of semi-structure interview. Therefore, the result, there are a consistency found between the findings of literature review and the findings of semi-structured interview that's aim to identify the security knowledge constructs to influence the employee behaviour in order to answer the first research question. Based on the above the security knowledge construct to influence the employee behaviour were identified.

For further explanations, semi-structured interview with the five information security experts were conducted, compiled, summarized, analysed, and then interpreted. For the analysis, the interviewees' responses were compared to the security knowledge constructs identified by the literature review so that the security knowledge constructs can be explored and confirmed through the interviewees. The responses obtained from the interview is also used to identify other knowledge required to influence employee behaviour in organisations. A summary of the findings of the semi-structured interviews is presented in this section.

In section 2.8, the security knowledge's constructs have been identified as knowledge of security threat, knowledge of organisation information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture related to security filed, knowledge of security responsibility and knowledge of security risk. It is pertinent for an organisation's employees to be informed of the above knowledge to enhance their security knowledge and ultimately, their behaviour. As mentioned, the interviews were conducted with a group of information security experts to get in depth understanding the constructs of security knowledge and their sufficiency to enhance employee behaviour. The content of the knowledge are explored to determine answers to the research questions. This phase is geared towards gaining information on the answer to RQ1 and evaluating the extensiveness of security knowledge in enhancing employee behaviour. The interview questions were developed to elicit the maximum information of the perceptions and the experience of the experts on information security. The interview questions are attached in Appendix D.

The interviews findings revealed that the six items of security knowledge constructs namely knowledge of security threat, knowledge of organisation information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility and knowledge of security risk are all relevant to help improve the employee behaviour in organisations by reducing internal security incidents and minimizing the risk posed by the insider.

A summary of the findings of the semi-structured interviews for each security knowledge constructs is presented in the following sub-sections.

4.7.1 Knowledge of Security Threat

The employees inside the organisation must understand the threats, type of threats and threats and the negative consequences of the threats towards organisations information assets. Furthermore, their knowledge must cover knowledge of perceived threat, with the latter referring to the level of the individual's perception of the danger and harmful nature of the threat. This knowledge is a combined version of knowledge of threat perceived severity and knowledge of threat perceived susceptibility, indicating that perceived threat covers perceived severity and perceived susceptibility. Some of the answers from the interviewee transcripts include the following:

"*Of course, the employees have to understand the threat and their types to behave cautiously when interacting with the information assets of the organisation. They have to* *understand and be knowledgeable on the threats to display a positive behaviour in protecting the organisation from within*" (Interviewee 2).

Similarly, according to interviewee 3:

"*In the current era of social engineering, some people impersonate others to obtain confidential information from employees and this necessitates that employees should have knowledge on the social engineering types like diving and faking. They must also have knowledge on threats and top cyber security for protection*".

Moreover, one of the interviewees mentioned:

"*Majority of the employees in the organisation use their smartphones and both smartphones and IOS are not secure in terms of downloading applications and connecting mobiles to internet. It is crucial to have anti-viruses in such tools. It is crucial for employees to be aware of email-security risks in the form of spamming, threats and phishing so that they won't fall for the cyber attackers traps*" (Interviewee 4).

According to interviewee 5, the top organisational threat from within is that employees who refuse to follow the policies of the organisation:

"*The major threat to the organisation is that employees refuse to follow the organisation's policy because they feel that this may take time and prevent natural flow of business work. However, security knowledge is important to them and they have to understand this and behave in a secure manner*".

Based on the interview findings, security threat related to type of threats, negative consequences of threats, perceived threat and harmful nature of the threat, threat perceived severity and threat perceived susceptibility. Hence, the knowledge of security threat is important to organisation employees and they have to understand to behave in a secure manner. Therefore, the instil knowledge of security threat between the employees help to influence their behaviour when they interacting with organisation information assets.

4.7.2 Knowledge of Organisation Information Security Strategy

The organisation information security strategy furnishes the suitable implementation of various information security strategies like plans of actions, policies, objectives, best practices, standards, guidelines and priorities that guide employees to accomplish goals to safeguard information assets.

According to interviewee 1:

"*The employees must be aware and understand the information strategies policy established by the organisation. To supplement this, the organisation can train employees and promote their awareness of information security issues*".

Along a similar line of answer, interviewee 2 mentioned:

"*We train employees on password policy, how to keep their passwords confidential and such training teaches them general security issues and the security techniques used within the organisation to influence their behaviour*".

Also, interviewee 4 said:

"*The provided awareness training primarily aims to make employees aware of cyber security policy of the company; for instance, the password policy mandates that passwords must be changed every 90 days and they should include alphabetic and numeric letter. Passwords are also mandated by the policy to be kept confidential and not shared with others. This all assists employees to understand the security policy of the company*".

Hence, the findings highlighted that the organisation information security strategy in terms of organisation security of plans, actions, policies, objectives, procedures, best practices, standards, guidelines and priorities that guide the employees behaviour to protect the organisation assets from inside. Therefore, the employee have to be trained and understood them to follow the organisation security strategy through providing a training awareness based on this security knowledge construct.

4.7.3 Knowledge of Security Technology

In this study's context, knowledge of security technology refer to knowledge concerning hardware, software, services, appliances and applications employed by the organisation for the protection of information assets. Disseminating knowledge concerning security technology has a key role in influencing and enhancing employees' behaviour towards protecting the organisation from within.

Interviewee 3 explained:

"*We instruct employees on basic IT security; for instance, cyber security elements, and the existing company security policy. We also make them aware of the technology types like antivirus software, firewall, and the presence of Trojan in the system. This training and instructions attempt to help them learn the general security issues and the techniques used in the organisation*".

Interviewee 4 said:

"*The company's security technology hardware, measures, firewall and antivirus have to be effectively implemented and the knowledge of employees concerning them will assist in protecting the company*".

Also, interviewee 5 said:

"*We instruct the employees on technology basic; for example of the technology types like antivirus software must be updated, the hardware technology that must be implemented to protect the organisation. These instructions will help them to behave in a secure manner*".

The interview findings showed that the instilling knowledge of security technology in terms of hardware, software, services, appliances and applications employed by the organisation for the protection of information assets has a key role in influencing and enhancing employees' behaviour towards protecting the organisation assets. Knowledge of security technology is one of security knowledge construct required to influence the employee behaviour. As a result, the organisation have to instruct the employees regarding on technology basic and technology types. The lack of sufficient knowledge of employees on policy usage of technology may lead to ineffective use of them and may do more harm than good to the organisation.

4.7.4 Knowledge of Legislation, Regulation and National Culture

The organisation's external environment and national culture significantly impact its information security culture. According to McIntosh (2011), organisations develop their information security assumption on the basis of their social values reflecting the environment. Stated clearly, the legislation, regulation, and national culture of the environment within which the organisation is run have to be considered when designing the organisation's structure, its information security culture, and security of information assets (Hogail, 2015).

According to interviewee 1:

"*It is a must for the employees to understand the national rules, regulations and legislations for the protection of the assets of the organisation. These include data protection act, HIPPA and privacy laws. These laws are good for the organisation to adopt for it to be able to protect its system*".

Similarly, interviewee 2 explained:

"*Employees have to be knowledgeable on the data protection act, privacy laws, and the regulation relating to data protection and individual rights in their country; these knowledge help them to act in a secure way".*

Interviewee 5 also mentioned:

"*Employees have to be knowledgeable on the national culture, legislation and regulations relating to data protection and individual rights including privacy laws, copyright laws, protection laws and intellectual property laws for themselves and for the organisation they work for. This knowledge is pertinent in influencing employees' behaviour*".

Based on the interview outcomes, employees have to be knowledgeable on legislation, data protection act, privacy laws, and the regulation relating to data protection and individual rights in their country, these knowledge help them to act in a secure way. As a result, knowledge of legislation, regulation and national culture help to influence the employee behaviour.

4.7.5 Knowledge of Security Responsibility

The employees working for the organisation is deemed to form the core of its information security culture on account of their important role in protecting information in the information security process (Da Veiga et al., 2007; Eloff & Eloff, 2005; Van Niekerk & Von Solms, 2010). Information security primarily aims to facilitate employees' behaviour to work towards the security of information assets, from the top management level to the most menial worker (Paulsen & Coulson, 2011). One of its main goals is to establish that information security is the responsibility of every employee, in that the knowledge of security responsibility has to be inculcated in each employee in order to protect the organisation from within. AlHogail (2015) stressed that information security responsibility has to consider every human factor to enhance user behaviour.

According to interviewee 2:

"*Security is rife with limitation when it comes to employees, and for the employees to follow security protocols, they need to understand them and to know their security responsibility*".

Also, interviewee 3 explained:

"*It is important for employees to understand and to obtain sufficient security knowledge on IT security in order to behave securely. For instance, if they are not aware that passwords have to be changed every few months, they should be instructed and told the reason why. They should be informed why passwords should include lower and upper case letters, and the security protocols in detail. They should be informed not to download from the Web, and they should be convinced that they have a security responsibility towards securing the organisations valuable assets*".

Interviewee 4 also explained:

"*Security of mobile devices like smartphone and IOS is very crucial, and employees have to be instructed to install anti-virus in their mobiles and not to install risky programs. The mails are also configured by the mobile tools therefore, email security from threats like spam, phishing, password and fake links have to be kept in mind. Security responsibility is crucial to employees and they must be aware of their responsibility towards data protection*".

Based on the interviews findings, security responsibility is crucial to employees and they must be aware of their responsibility towards data protection. Hence, inculcating knowledge of security responsibility between the employees can help to reduce the internal security incidents within an organisation. As a result, knowledge of security responsibility help to influence employee behaviour.

4.7.6 Knowledge of Security Risk

Knowledge of security risk aims to promote employees' awareness of security risks and their responsibilities towards security that drive them towards acting in a secure way (Da Veiga & Eloff, 2010; Parsons et al., 2015). Additionally, it assists employees to know, understand and adopt the required precautions and ensure that they possess the required skills for appropriate actions (Furnell et al., 2010), and for the pursuant of secured behaviour.

Inculcating knowledge of security risk to employees works towards safeguarding them, the organisation and the information assets of the organisation. It will also make them aware of the potential risks, which in turn, would affect their behaviour and adopted actions.

According to the interviewee 1:

"*Email security awareness covers awareness of spams, Trojan attachments or phishing online. It also includes awareness of risks when accessing emails from unknown senders and accessing of the internet. These should all be known by the employees it should be ensured that they have knowledge on information security culture*".

Moreover, interviewee 4 stated:

"*It is important for employees to be aware of risks in accessing emails and issues of security in this regard include spam, phishing online, email passwords and fake links*".

Furthermore, interviewee 5 expounded on his answer to the question:

"*Email security awareness is to be aware of spams, Trojan attachments or phishing online. It is crucial that employees are aware of risks when accessing emails and the risks of accessing the internet. It is also crucial for them to known security risks that can assist in influencing their behaviour*".

The interviews revealed, it is crucial to educate employees and alert them on the risks and dangers stemming from the environment that surrounds information assets and the risks that may occur when going through an unsecured behaviour within the organisation. Inculcating knowledge of security risk to organisation employees aims to guide the employee behaviour when interacting with information assets, which in turn, would affect their behaviour and adopted actions.

4.7.7 Security Knowledge Constructs with Six Items

Majority of the interviewees stress on the constructs of security knowledge and their validity to enhance employee behaviour within organisations. They also stated that this knowledge is comprehensive, valid and significant for the enhancement of employees' behaviour. All of them are of the consensus that all the knowledge constructs have positive influence on the behaviour of employees; for instance, one interviewee said that:

"*These types of security knowledge are crucial for the employees to know for them to manage their behaviour*" (Interviewee 1).

In addition, another interviewee mentioned:

"*If these knowledge aspects are inculcated to the employees of the organisation, they will effectively influence their behaviour*" (Interviewee 2).

Interviewee 3 also supported this by saying:

"*Of course, if the employees know and understand security knowledge, it will definitely have a positive influence on their behaviour during their interaction with the information assets of the organisation*".

Similarly, interviewee 4 confirmed:

"*It is without a doubt that these security knowledge constructs are sufficient for the secure behaviour of employees, so that employees will positively behave if they have knowledge about them*".

Lastly, according to interviewee 5:

"*If the employees understand and known information security, they will act in a secure manner and display better behaviour*".

The interviews findings revealed that the six items of security knowledge constructs namely knowledge of security threat, knowledge of organisation information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility and knowledge of security risk are all relevant to help influence the employee behaviour in organisations by reducing internal security incidents and minimizing the risk posed by the insider.

4.8 Summary

This chapter presents the qualitative analysis and findings from actual interviews. Six items of security knowledge has been confirmed by the five information security experts that have been interviewed; two of them from academicians, while the others are information security in organisations.

Finally, the last part of the chapter discussed the findings obtained from the interviews through a qualitative analysis. All the interviewees confirmed that these security knowledge constructs is complete and comprehensive which contains the most of security knowledge that must be implemented between the employee to influence their behaviour and to protect the organisations assets.

CHAPTER 5

RESEARCH MODEL AND HYPOTHESIS DEVELOPMENT

5.1 Introduction

In this chapter, the stepwise formulation of the research model is presented and the hypotheses are developed and explained. Section 5.2 presents the KAB model selection and justifications. Section 5.3 presents the adapted KAB model. Section 5.4 presents the variables of the adapted KAB model. Section 5.5 discusses the research variables and hypotheses development in this research. Finally, section 5.6 presents the summary of this chapter.

5.2 KAB (Knowledge-Attitude- Behaviour) Model Selection and Justification

This study primarily aims to develop a model that determines the knowledge-behaviour relationship and the impact of each security knowledge constructs on the behaviour under question. Studies of the literature have revealed positive relationship between knowledge and behaviour. In this study, security knowledge is extended to six constructs to influence the employee security behaviour. The constructs are then confirmed by a group of security experts to support the findings obtained from the literature review. The constructs of security knowledge should be employed in the organisation for the enhancement of employee behaviour based on their relationship with the information assets of the organisation. A research model is proposed to examine the relationship between knowledge-behaviour in this context, and from this examination, hypotheses are formulated addressing the relationship between the constructs of security knowledge and behaviour in terms of the former's impact on the latter.

The knowledge-behaviour relationship is examined by extensively investigating specific models/theories. The KAB model is the most suitable model to represent the interconnection among knowledge, attitudes and behaviour as presented by Kruger & Kearney (2006). The KAB model can help to determine the above mentioned interconnections and to determine the effects of security knowledge on behaviour under question.

In this regard, Kruger & Kearney (2006) created a prototype model to measure information security awareness in an international gold mining firm, and measured the information security awareness program's effectiveness based on knowledge, attitude and behaviour. In relation to this, knowledge affects the attitude of an individual towards a particular behaviour, and in turn, an attitude enhance the desired behaviour (Ajzen, 1991; Armitage & Conner, 2001). The above concepts are referred to as the Knowledge-Attitude-Behaviour (KAB) model (McGuire, 1969).

There are several reasons why KAB model used to represent the knowledge-attitude-behaviour relationships in this research:

(1) Many studies such as Kaur & Mustafa (2013); Parsons et al. (2014, 2015); Veseli (2011) that assessed the effectiveness of security awareness program. They employed the KAB model to assess the effectiveness of the security awareness programs for the organisation's employees. This is similar to this research work, which concentrates on the importance of security knowledge construct in the organisation to reinforce the security awareness programs that enhances the employee behaviour with in organisations. Specifically, it helps to concentrates on security knowledge constructs that must be instilled between the organisation employees to influence their behaviour.

(2) The human factor in information security comprises of two dimensions and they are knowledge and behaviour, both of which are interrelated. The positive relationship assumption between knowledge and behaviour is backed by the reviewed literature. The KAB model represent the relationship between knowledge, attitude and behaviour. Studies have shown that there is a relationship between knowledge and attitudes, attitudes and behaviour, and knowledge and behaviour. It is those literatures that confirmed these relationship and the validity of the KAB model.

(3) This research aims to determine the impact each of security knowledge constructs on behaviour based on the knowledge-attitude-behaviour relationship. The KAB model clearly represent these relationship.

This study is an attempt to determine the security knowledge constructs that enhance and extend knowledge among employees and contribute to influence the employee behaviour. It also aims to identify the impact of each security knowledge constructs required to bring about the behaviour in question. The focus is thus on knowledge more than behaviour and thus, the knowledge has been extended in KAB model to include security knowledge constructs such as knowledge of security threat, knowledge of security technology, knowledge of organisation security policy, knowledge of security responsibility, knowledge of security risk, knowledge of legislation, regulation and national culture.

The KAB model is primarily concerned with the knowledge aspect of the individual (Baranowski, Cullen, Nicklas, Thompson & Baranowski, 2003; Kruger & Kearney, 2006). The KAB model posits that knowledge is gathered over time of a relevant behaviour; for instance, in different fields such as information security, health, environment, education information, among others, initiate change in attitude. The model sheds light on the knowledge role in behavioural change and the knowledge accumulation, with such knowledge accumulation leading to changes in attitude, and ultimately, changes in behaviour. There are several studies that used KAB model to determine the knowledge-attitude-behaviour relationship in various fields and domains and these include ones conducted by Kaur & Mustafa (2013). The authors conducted an evaluation of the information security awareness among employees in SMEs (Small Medium Enterprise) by examining the relationship among the constructs. They used partial least square (PLS) based on KAB theory. Similarly, (Khan, Alghathbar, Nabi & Khan (2011); Kruger & Kearney (2006) contended that users possessing the right knowledge are more capable of preventing threats and attacks, and this increases the confidentiality, integrity and availability of information. They found significant relationship between users' attitude and behaviour, and information security awareness, but no significant relationship between knowledge and information security awareness. The findings also showed that attitude and behaviour were significantly related to confidentiality, indicating that employees know their responsibilities when it comes to keeping business information and resources. The users did not have the required knowledge to handle information security issues like phishing email. The non-significant relationship of knowledge may be attributed to this. To this end, it is crucial for organisations to educate their employees and enhance their knowledge on information security.

Viewed from the field of social psychology, Kruger & Kearney (2006) created a prototype to measure information security awareness with the use of knowledge, attitude and behaviour (KAB) model. The underlying premise of the KAB is the understanding of the relationship between the three components, revealing that with the accumulation of knowledge in a certain behaviour, (information security, health, education), changes are eventually initiative in attitude that will increasingly change the behaviour in question.

The KAB and theory of planned behaviour (TPB) was employed by Khan et al. (2011) to examine the effectiveness of information security awareness approaches. The proposed model was based on the knowledge attribute adopted from KAB, and attitude and social norms from the TPB Fishbein & Ajzen (1977) to accomplish the required behavioural change. The obtained findings indicated the ability to change the behaviour of users and thus, promote the awareness of users concerning information security.

In a related study, Veseli (2011) assessed and measured the effectiveness of information security awareness program, with the help of KAB model. He found that awareness programs best affects and enhances user's knowledge, attitude and behaviour towards information security. They contended that information security awareness initiatives positively affect the knowledge, attitude and behaviour of employees in actual workplaces. Moreover, in der Linden (2012) study, the author reviewed past studies dedicated to climate change and revealed considerable evidence supporting the significant relationship among the constructs of environmental knowledge, attitudes and behaviours.

Meanwhile, the KAB model's relevance to the promotion of health was examined by Bettinghaus (1986) after which they reached to the conclusion that there is a positive but small relationship between knowledge, attitude and behaviour.

Moreover, a small-medium positive relationship was also reported by Parsons et al. (2015) between organisational information security culture and employees' information security decision making. In particular, employees from organisations having optimum information security culture had a greater tendency to have knowledge, attitudes and behaviours that adhere to information security policy and procedures. This shows that enhancing organisational information security culture in organisations could lead to enhanced adherence to its established policy and procedures. This could then assist in minimizing human-based cyber risks in the organisation.

5.3 Adapting the KAB Model

Based on the literature review conducted on the use of KAB model in information security, the KAB model developed by Kruger & Kearney (2006) has been used to represent the relationship between knowledge and behaviour. In KAB model, three components were used as a basis and the model was developed on three equivalent dimensions namely what does a person know (knowledge); how do they feel about the topic (attitude); and what do they do (behaviour) (Kruger & Kearney, 2006).

In this study, security knowledge is extended to include security knowledge constructs that are discussed in section 2.4.3 in order to identify the security knowledge required to influence the employee behaviour. Therefore, the knowledge in KAB model as shown in Figure 5.1 has been extended to include security knowledge constructs such as knowledge of security threat, knowledge of security technology, knowledge of organisation security policy, knowledge of security responsibility, knowledge of security risk, knowledge of legislation, regulation and national culture. The KAB research model was adapted to include security knowledge construct in order to define the relationship between security knowledge constructs, attitudes and behaviour, and on this basis, the hypotheses were developed to determine the impact each of security knowledge construct on behaviour.

\

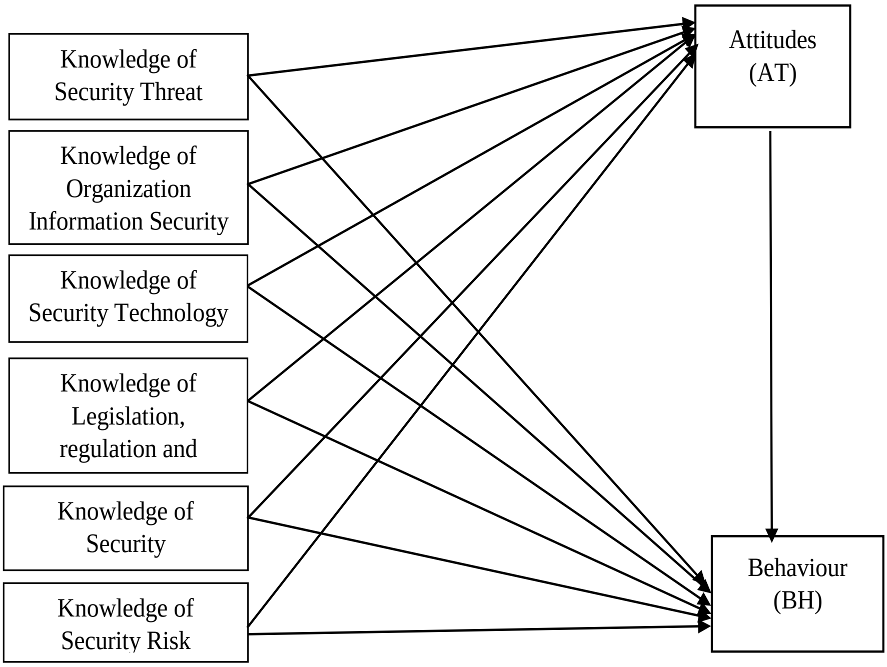

Knowledge of Security Threat
Knowledge of Organization Information Security
Knowledge of Security Technology
Knowledge of Legislation, regulation and
Knowledge of Security
Knowledge of Security Risk
Attitudes (AT)
Behaviour (BH)

Figure 5.1 Adapted KAB model

The relationship between knowledge, attitude and behaviour in the adapted KAB model is shown in Figure 5.2. In this model, knowledge affects the attitude of an individual towards a particular behaviour, and in turn, an attitude enhance the desired behaviour. The model sheds light on the role of knowledge in behavioural change and the knowledge accumulation, with such knowledge accumulation leading to changes in attitude, and ultimately, changes in behaviour. In other words, with the accumulation of knowledge in a certain behaviour such as security behaviour, changes eventually occur in attitude that will increasingly change the behaviour in question. It is clear that if employees can interpret or understand security policy and the relevant documents, they can behave in accordance with official security policies. They can perform security activities accordingly and their security behaviours would become visible. Visible security behaviours are important because they can be good examples of security practices which can inspire everyone in the organisation. In an ideal situation, once employees know how to perform security activities in their daily work routine, then security practices can become entrenched within the organisation, which in turn can help to influence their behaviour and cultivate an appropriate security perception amongst the employees.

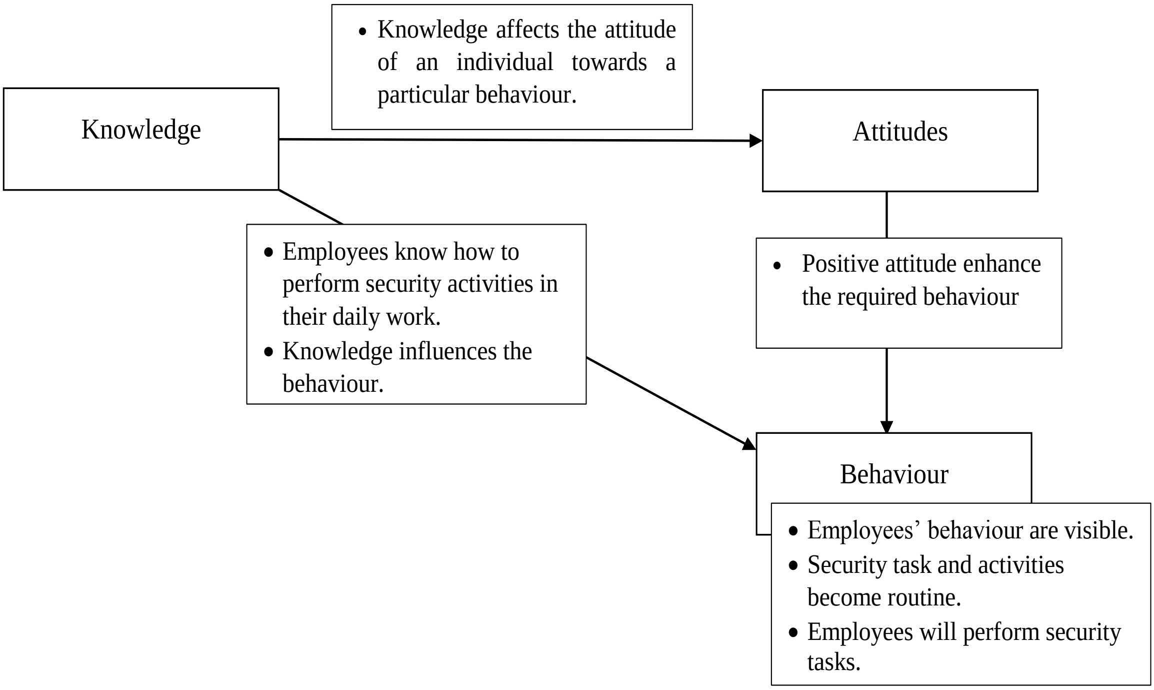

Knowledge affects the attitude of an individual towards a particular behaviour.
Knowledge
Attitudes
Employees know how to perform security activities in their daily work.
Knowledge influences the behaviour.
Positive attitude enhance the required behaviour
Behaviour
Employees' behaviour are visible.
Security task and activities become routine.
Employees will perform security tasks.

Figure 5.2 The relationship between knowledge, attitude and behaviour in the adapted KAB model

5.4 Variables of the Adapted KAB Model

In the previous sections, the KAB model has been presented and extended to include the relevant knowledge constructs so that relationship between various types of security knowledge and behaviour can be represented. In this section, the variables of each elements in KAB model such as knowledge, attitude and behaviour are identified and analysed using content analysis based on the literature review and the findings of semi-structured interview that conducted in this study in order to confirm, explore and to get in-depth understanding about variables and principles of security knowledge constructs (Chapter four). The following table present the variables for each element in KAB model.

Table 5.1 Summary of Variables in Knowlege, Attitude and Behaviour in adapted KAB model

Security Knowledge (Security Knowledge Construct)	**Attitude** (Attitude toward Security Knowledge Construct)	**Behaviour** (Security Behaviour)
- Knowledge of Security Threat - Knowledge of Organisation Information Security Strategy - Knowledge of Security Technology - Knowledge of Legislation, regulation and National Culture - Knowledge of Security Responsibility - Knowledge of Security Risk	- Necessary to know - Important - Benefit - Help to mitigate the risk. - Valuable - Positive effect to protect - Minimize the risk. - Influence behaviour - Guide behaviour.	- Update anti- virus regularly. - lock computer. - Clear disk policy. - Repot security incidents. - What to protect. - What to do. -Share Information - Follow organisation policy. - Prevent, detect, respond and reflection. - Follow organisation security policy. - Manage password regularly. - Protect confidential information. - Don’t open attachment from unknown sender.

These variables help to get in depth understanding the elements of knowledge, attitude and behaviour in KAB model that aims to direct the employee behaviour and help to find a suitable appropriate security perception between the employees in order to minimize the internal security incidents, to minimize the risk of exposure of information assets and help to determine the impact relations between knowledge, attitude and behaviour.

5.5 Research Model and Hypothesis Development

In this section, the adopted process entailed in developing a theoretical model is explained. This is crucial for hypothesizing the logical relationships between the significant constructs, with the aim of examining the research problem. Following the development of the model, the hypotheses were formulated to investigate the relationships. Hypothesis testing is important in achieving the primary study objectives, which is to determine the effects of security knowledge construct on the behaviour of employees.

5.5.1 Hypothesis Development

This section presents the development of the study hypotheses based on the relevant studies reviewed in the literature. Testing hypotheses determines the relationships between different variables that are important to the study, and in the present one, the relationships among knowledge, attitude and behaviour based on KAB are the main focus.

In this study, the knowledge in KAB model as shown in Figure 5.3, has been extended to include security knowledge constructs such as knowledge of security threat, knowledge of security technology, knowledge of organisation security policy, knowledge of security responsibility, knowledge of security risk, knowledge of legislation, regulation and national culture. The KAB research model was adapted to include security knowledge construct to define the relationship between security knowledge constructs, attitudes and behaviour, and on this basis, the hypotheses were developed.

On the basis of the above variables, the study hypotheses were developed in the research model to determine the impact of security knowledge constructs to employee behaviour. The proposed relationships are then tested and confirmed using an organized progression of examination.

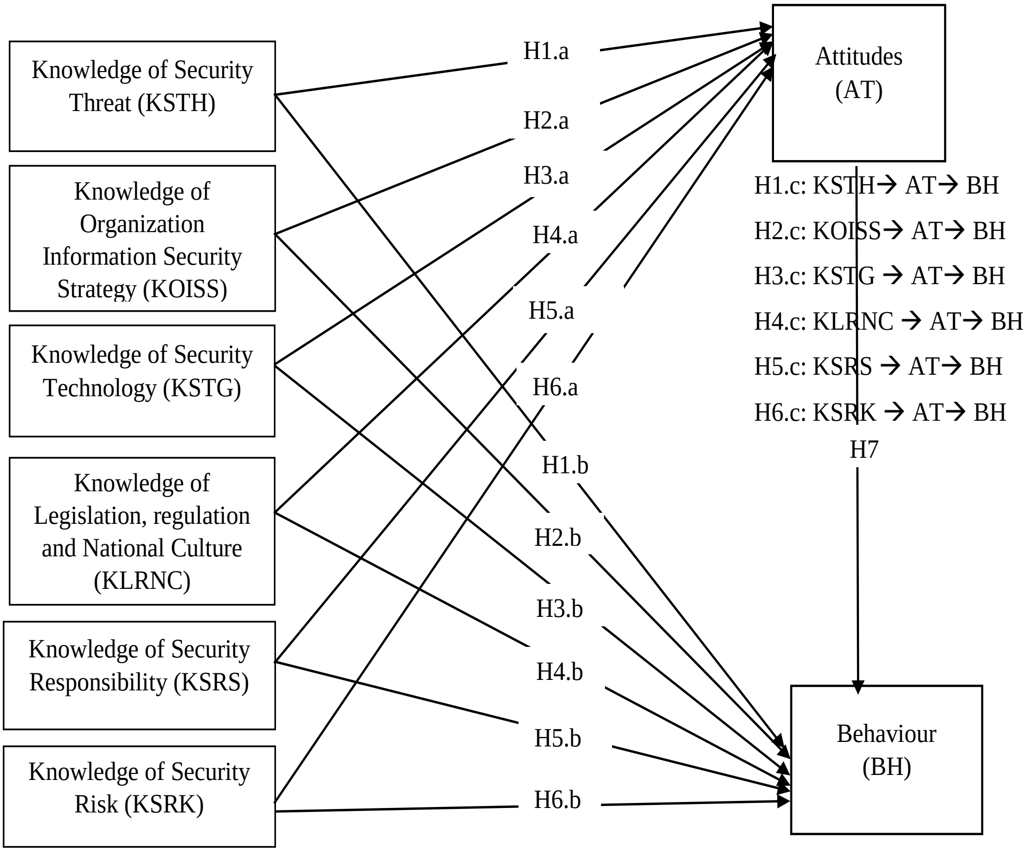

Knowledge of Security Threat (KSTH)
Knowledge of Organization Information Security Strategy (KOISS)
Knowledge of Security Technology (KSTG)
Knowledge of Legislation, regulation and National Culture (KLRNC)
Knowledge of Security Responsibility (KSRS)
Knowledge of Security Risk (KSRK)
H1.a
H2.a
H3.a
H4.a
H5.a
H6.a
H1.b
H2.b
H3.b
H4.b
H5.b
H6.b
Attitudes (AT)
H1.c: KSTH→ AT→ BH
H2.c: KOISS→ AT→ BH
H3.c: KSTG → AT→ BH
H4.c: KLRNC → AT→ BH
H5.c: KSRS → AT→ BH
H6.c: KSRK → AT→ BH
H7
Behaviour (BH)

Figure 5.3 The proposed research model

5.5.1.1 The Relationship between Knowledge and Behaviour

Several studies in literature have been dedicated to studying the knowledge-behaviour relationship (Areej Al Hogail, 2015; Rashid et al., 2013; Liebowitz & Wilcox, 1997; Zakaria, 2006; Spijkervet 2005; Van Niekerk & Von Solms, 2010; Topa & Karyda ,2015). The findings showed a positive relationship between security knowledge levels and employees' behaviour.

In information security, the human factor comprises of two dimensions and they are knowledge and behaviour and both are interconnected (Van Niekerk & Von Solms, 2010). It is crucial for employees to be aware of the importance of information security so that they may safeguard the assets of the organisation. In other words, it is crucial for them to understand and apply security knowledge in order to display the right behaviour when it comes to the concept. In this regard, knowledge should match behaviour in order for the desired behaviour to be achieved within the organisation.

Moreover, security behaviour is described as the ability of the employee to adopt the suitable and effective security actions (Blythe et al., 2015). Behaviour is the assumption about what behaviour regarding the protection of information is encouraged or not (Van Niekerk & Von Solms, 2010) .

On the other hand, knowledge refers to the theoretical and practical understanding of the subject, fact, information, value or skill accomplished via education or experience (Sohrabi Safa et al., 2016). Knowledge has its basis on user knowledge on the right behaviour to adopt in specific situations (Kruger & Kearney, 2008). It has the ability to increase the required behaviour relating to information assets of the organisation. On the basis of the ability to know and understand the constructs of security knowledge, it is crucial for the employees to know the security threats in the form of viruses, spam email, downloading suspicious software, phishing issues, scan attachment in emails and access trusted sites. Furthermore, employee must know how to have strong passwords, do not share password between others, and change it constantly based on the policies of the organisation. Employee must know and understand security knowledge construct as illustrated in Section 2.8 (e.g., security technology knowledge, security responsibility knowledge, security of risk knowledge, and knowledge regarding legislation and national culture. Employees having the right knowledge concerning security knowledge constructs are expected to be able to manage behaviour and safeguard the information assets of the organisation. On the basis of the discussion above, the following hypotheses are formulated, which are depicted in Figure 5.3.

The knowledge of security threats among the employees in the organisation has a positive impact on their behaviour and thus the following hypothesis is proposed to be tested;

H1b: *There is a significant relationship between knowledge of security threat and behaviour*.

The knowledge of organisational information security strategy among the employees in the organisation has a positive impact on their behaviour and thus the following hypothesis is proposed to be tested:

H2b: *There is a significant relationship between knowledge of organisation information security strategy and behaviour*.

Moreover, the knowledge concerning the technology among all the employees in the organisation has a positive impact on their behaviour and thus,

H3b: *There is a significant relationship between knowledge of security technology and behaviour*.

Also, the knowledge concerning legislation, regulation and national culture of all the employees in the organisation positively impacts their behaviour and thus, the following hypothesis is proposed to be tested;

H4b: *There is a significant relationship between knowledge of legislation, regulation and national culture, and behaviour*.

The employees' knowledge on security responsibility positively impacts their behaviour and therefore,

H5b: *There is a significant relationship between knowledge of security responsibility and behaviour*.

Lastly, knowledge of all employees concerning security risk has a positive effect on their behaviour and thus, the following hypothesis is proposed;

H6b: *There is a significant relationship between knowledge of security risk and behaviour*.

5.5.1.2 The Relationship between Attitudes and Behaviour

The attitude-behaviour relationship has been examined with the help of several theories, like the Theory of Planned Behaviour (TPB), a theory developed by Ajzen (1991) from the Theory of Reasoned Action (TRA). The TPB focuses on improving the compliance behaviour of individuals through their attitudes, perceived behavioural control and subjective norms – these constructs influence the intention of individuals towards a specific behaviour(Safa & Von Solms, 2016).

In addition, the attitudes-behaviour relationship was extensively studied in literature; for instance, Al-umaran (2015) investigated and analysed the effect of cultural dimensions on the Saudi information security in the context of the health service. The author based the study's conceptual framework on the theory of human behaviour, with the attitude of the individual being the major element of his behaviour. The Human Behaviour theory posits that the individual's attitude is the major component forming his intention to behaviour and his actual behaviour.

In a study of the same calibre, Pattinson et al. (2016) assessed information security attitudes among university students, focusing on participants' attitudes towards accidental information security behaviour among university students. Their theoretical framework was based on Ajzen's (1991) theory of planned behaviour (TPB). They recommended further studies to understand the employees' attitudes towards behaviours. Also, Blythe et al. (2015) focused on the underpinning behavioural contexts of information security in the workplace, and explored the way individual and organisational factors influence the interactions of the motivations and barriers of security behaviours. The analysis findings showed a positive relationship between attitudes and behaviour and a positive relationship between knowledge and behaviour.

Employee behaviour can change based on one's attitude. Behaviour that is liked or disliked, desirable or undesirable, good or bad, or behaviour that is viewed positively or negatively

(Pattinson et al., 2016). Many studies support the relation between attitudes and behaviour. This suggests that attitude may be an important antecedent of security behaviour. This context shows that the attitudes of employees on knowledge and understanding the constructs of security knowledge required positively impacts their behaviour. On this basis, the study proposes the related hypotheses based on Figure 5.3.

The attitude of employees towards security knowledge required in the organisation positively impacts their behaviour and thus;

H7: *Employees' attitude towards security knowledge required has a positive effect on their behaviour.*

5.5.1.3 The Relationship between Knowledge and Attitudes

In this section many definitions of attitude is presented, such as; attitude is described as the positive or negative feeling towards a given behaviour and it is defined as the learned inclination to evaluate things in a certain way (Liang & Xue, 2009). Such evaluation may be positive or negative regarding an object, issue, people or events (Leonard, Graham, & Bonacum, 2004). Attitude stems from the past and present of the individual and it is often related to as the evaluation of objects, people, activities, events and ideas ranging from extremely positive to extremely negative. It is also described as the individual's positive or negative view concerning his engagement with a specific behaviour. According to Hepler (2015), attitude is a psychological inclination that ranges from extremely negative to extremely positive ends. The attitude concept has attracted the attention of many experts in the different domain, because of its potential to describe an individual's behaviour.

Majority of studies revealed the existence of knowledge-attitude relationship (e.g., Kruger & Kearney (2006); Khan et al., (2011); (Veseli, 2011); der Linden (2012); (Bettinghaus, 1986); Parsons et al. (2015)). Some authors found a significant relationship, whereas others indicated a moderate one. To protect critical information assets, promoting a campaign on security education assists in modling attitudes and behaviours of managers and employees (Wilson & Hash, 2003).

Knowledgeable employees who are privy to the security knowledge constructs tend to have a positive attitude towards safeguarding the information assets of the organisation. Hence, the following hypothesis is proposed as presented in Figure 5.3.

Security threat knowledge of the employees within the organisation has a positive impact on their attitude and therefore;

H1a: *There is a significant relationship between knowledge of security among employees and their attitudes*.

Knowledge concerning information security strategy of all the employees of the organisation has a positive impact on their attitude and therefore;

H2a: *There is a significant relationship between knowledge of information security strategy of employees and their attitudes*.

Moreover, knowledge of employee concerning security technology has a positive impact on their attitude and therefore, the following hypothesis is proposed;

H3a: There is a significant relationship between knowledge of security technology of employees and their attitudes.

Furthermore, the employees' knowledge of legislation, regulations and national culture has a positive impact on their attitude and thus, the following hypothesis is proposed to be tested;

H4a: *There is a significant relationship between knowledge of legislation, regulation and national culture among employees and their attitudes*.

Along a similar line of hypothesis development concerning knowledge of security responsibility among employees, such knowledge has a positive impact on employees' attitude, which leads to the following hypothesis;

H5a: There is a significant relationship between knowledge of security responsibility among employees and their attitudes.

Also, knowledge of security risk among all employees has a positive impact on their attitude. Therefore, it is hypothesized that;

H6a: There is a significant relationship between knowledge of security risk among employees and their attitudes.

5.5.1.4 The Relation between Knowledge, Attitude and Behaviour

When employees are provided with knowledge concerning security knowledge, this would work towards transforming their attitudes, assumptions, views and knowledge and will impact their behaviour in the organisation (Alhogail, 2015; Da Veiga & Eloff, 2010; Kaur & Mustafa, 2013) .

In fact, several studies have been dedicated to examining the knowledge-attitude-behaviour relationship. More specifically, Veseli (2011) assessed and measured the effectiveness of information security awareness initiative using KAB model. He found that such initiatives influence and enhance the knowledge, attitude and behaviour of users towards information security. Generally speaking, information security awareness companions positively impact the actual working environment of employees in terms of their knowledge, attitude and behaviour.

In a related study, der Linden (2012) looked into the area of climate change and indicated ample evidence to support a significant environmental knowledge-attitudes-behaviours relationship. Meanwhile, in a study by (Bettinghaus, 1986), the author made use of the KAB model to examine health promotion and found a positive but small relationship between the three constructs mentioned above.

Similarly, a small-to-moderate positive relationship was reported between organisational information security culture and aspects of employees' information security decision-making by Parsons et al. (2015). In other words, organisations possessing optimum information security culture had a higher tendency for employees to have knowledge, attitudes, and behaviour that is aligned with the information security policies and procedures. This indicates that enhancing the security knowledge could improve adherence of employees to policy and procedures and minimize human-based cyber risks.

More importantly, the employees' security knowledge construct assumed to have a positive indirect impact on their behaviour via attitude, where attitude mediates the relationship between security knowledge constructs and behaviour. Thus, the employees' knowledge on security threat is assumed to have a positive indirect impact on their behaviour via attitude, where attitude mediates the relationship between knowledge of security threat and behaviour. Therefore, as presented in Figure 5.3, the following relationship is hypothesized:

H1c: Attitudes (AT) of employees mediate the relationship between their knowledge of security threat (KSTH) and their behaviour (BH).

In relation to the above hypothesis, the knowledge of organisation's information security strategy among employees is assumed to positively and indirectly impact on their behaviour via attitude. Stated clearly, attitude is hypothesized to mediate the relationship between knowledge of organisation information security strategy and employees' behaviour, which leads to proposing the following hypothesis;

H2c: Attitudes (AT) among employees mediate the relationship between their knowledge of organisation information security strategy (KOISS) and their behaviour (BH).

This holds the same for the knowledge of security technology among employees and the presence of its positive and indirect impact on employee behaviour via attitude. Attitude mediates the relationship between knowledge of security technology and behaviour and therefore, this study proposes the following hypothesis for testing;

H3c: Attitudes (AT) among employees mediate the relationship between their knowledge of security technology (KSTG) and their behaviour (BH).

Moreover, knowledge of employees of legislation, regulation and national culture of the organisation positively and indirectly influences their behaviour via attitude. In other words, attitude mediates the relationship between knowledge among employees concerning legislation, regulation and national culture and their behaviour. Therefore, the following hypothesis is proposed to be tested;

H4c: Attitudes (AT) among employees mediate the relationship between their knowledge of legislation, regulation and national culture (KLRNC) and their behaviour (BH).

Furthermore, employees' knowledge on their security responsibility in the organisation has a positive and indirect impact on their behaviour through attitude, where attitude mediates the relationship between the first two constructs. Therefore, the following hypothesis is proposed to be tested;

H5c: Attitudes (AT) among employees mediate the relationship between their knowledge of security responsibility (KSRS) and their behaviour (BH).

Finally, the employees' knowledge on security risk positively and indirectly impacts their behaviour through attitude, where attitude mediates the relationship between the former two. Thus, the following hypothesis is proposed to be tested;

H6c. Attitudes (AT) among employees mediate the relationship between their knowledge of security risk (KSRK) and their behaviour (BH).

To sum up the hypothesis, Table 5.2 depicts the proposed hypotheses based on KAB model.

Table 5.2 Research Hypotheses Codes and Descriptions

Code	**Description**	**Path**
Direct Effect of Constructs		
H1.a	Knowledge of Security Threat (KSTH) has significant effect on Attitudes (AT)	KSTH → AT
H2.a	Knowledge of Organisation Information Security Strategy (KOISS) has significant effect on Attitudes (AT)	KOISS → AT
H3.a	Knowledge of Security Technology (KSTG) has significant effect on Attitudes (AT)	KSTG → AT
H4.a	Knowledge of Legislation, Regulation and National Culture (KLRNC) has significant effect on Attitudes (AT)	KLRNC → AT
H5.a	Knowledge of Security Responsibility (KSRS) has significant effect on Attitudes (AT)	KSRS → AT
H6.a	Knowledge of Security Risk (KSRK) has significant effect on Attitudes (AT)	KSRK → AT
H1.b	Knowledge of Security Threat (KSTH) has significant effect on Behaviour (BH)	KSTH → BH
H2.b	Knowledge of Organisation Information Security Strategy (KOISS) has significant effect on Behaviour (BH)	KOISS → BH
H3.b	Knowledge of Security Technology (KSTG) has significant effect on Behaviour (BH)	KSTG → BH

H4.b	Knowledge of Legislation, Regulation and National Culture (KLRNC) has significant effect on Behaviour (BH)	KLRNC → BH
H5.b	Knowledge of Security Responsibility (KSRS) has significant effect on Behaviour (BH)	KSRS → BH
H6.b	Knowledge of Security Risk (KSRK) has significant effect on Behaviour (BH)	KSRK → BH
H7	Attitudes (AT) has significant effect on Behaviour (BH)	AT → BH
Mediation Effects of Attitudes (AT)		
H1.c	Attitudes (AT) mediates the relationship between Knowledge of Security Threat (KSTH) and Behaviour (BH)	KSTH→AT→BH
H2.c	Attitudes (AT) mediates the relationship between Knowledge of Organisation Information Security Strategy (KOISS) and Behaviour (BH)	KOISS →AT→BH
H3.c	Attitudes (AT) mediates the relationship between Knowledge of Security Technology (KSTG) and Behaviour (BH)	KSTG →AT→BH
H4.c	Attitudes (AT) mediates the relationship between Knowledge of Legislation, Regulation and National Culture (KLRNC) and Behaviour (BH)	KLRNC →AT→BH
H5.c	Attitudes (AT) mediates the relationship between Knowledge of Security Responsibility (KSRS) and Behaviour (BH)	KSRS →AT→BH
H6.c	Attitudes (AT) mediates the relationship between Knowledge of Security Risk (KSRK) and Behaviour (BH)	KSRK →AT→BH

5.6 Summary

In this chapter, the formulation of the research model is discussed along with the introduction of the study hypotheses. Knowledge factor has been extended in KAB model into six constructs to cover the security knowledge constructs namely knowledge of security threat, knowledge of organisation information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility and knowledge of security risk. The KAB research model was adapted to define the relationship between knowledge, attitudes and behaviour, and on this basis, the hypotheses were developed.

CHAPTER 6

DATA ANALYSIS AND FINDINGS

6.1 Introduction

This chapter elaborates on the analysis conducted and establishes the empirical results to examine the research hypotheses, aided by AMOS 20 and SPSS 18 software. This chapter comprises of eight major sub-sections.

Section 6.2 presents the data screening. In this particular section, we elaborate on the procedures used to purify the data by way of substituting the missing values, discarding the outliers and testing the normality of data distribution. Section 6.3 offers a thorough explanation of the survey respondents and sample profile. Section 6.4 represents the measurement models' results via the Confirmatory Factor Analysis (CFA) that assess the constructs' uni-dimensionality, reliability and validity of the constructs. The descriptive results of the constructs are presented in section 6.5. In section 6.6 the results of the structural models that examine the hypothesized direct and mediation effects developed in this research are presented. Section 6.7 provides a discussion on the relation between security knowledge constructs, attitude and behaviour. Finally, section 6.8 summarises the data analysis results and the findings

6.2 Data Screening

Data screening is done to ensure that data are correctly entered, they do not have any missing values or outliers and that the normal distribution of variables can be confirmed. Appendix E highlights all the exogenous and endogenous variables as well as their relative estimation errors used in this study.

6.2.1 Replacing Missing Values

Missing data would be the case when respondents did not get to answer one or more items in the survey. The data screening indicates that there is little missing data (not more than 5%). Cohen (1983) points out that missing data up to 10% may not lead to any serious problem when interpreting the findings. To treat the missing data, recent literature suggests that Expected Maximisation (EM) is a better method to be adopted compared to other methods (Graham, Hofer, Donaldson, MacKinnon & Schafer, 1997) . However, since the missing data was minimal, the choice of method may not exert any significant influence on the results because each method has its own strengths and weaknesses (Hair et al., 1998). Therefore, these missing data were replaced with the variable median responses for each variable. This method is chosen because median substitution is the most commonly used method (Schwab, 2013) and it is one of the simplest methods for this purpose. With small amount of missing data, more complicated methods are not required.

6.2.2 Removing Outliers

The treatment of outliers would be a vital step to perform in the data screening method. Outliers denote the observations with a distinctive combination of characteristics identifiable as very different from the other observations (Hair et al., 1998). Outliers were identified using univariate and multivariate detections. Outliers need to be removed because they could affect the data normality which could then misrepresent the statistical results (Hair et al., 1998; Tabachnick, 2001).

6.2.2.1 Univariate Outliers

Each variable was examined for the standardised (z) score, for univariate detection, apart from examining histograms and box-plots. According to Hair et al. (1998), for large sample size above 200, Absolut (z) > 4 is evidenced of an extreme observation. The standardised (z) scores of the cases are summarized in table 6.1 for the items in each construct.

Table 6.1 Result of Univariate Outlier Based on Standardized values

Construct	*Item*	**Standardized value (Z-Score)**

		Lower Bound	Upper Bound
Knowledge of Security Threat (KSTH)	KSTH1	-2.143	1.701
	KSTH2	-2.182	1.732
	KSTH3	-2.363	2.034
	KSTH4	-2.372	1.941
	KSTH5	-2.276	2.101
Knowledge of Organisation Information Security Strategy (KOISS)	KOISS1	-2.028	1.755
	KOISS2	-2.062	1.892
	KOISS3	-2.084	1.855
	KOISS4	-2.030	1.936
	KOISS5	-2.001	1.772
	KOISS6	-2.045	1.790
	KOISS7	-1.947	1.936
	KOISS8	-1.972	1.750
	KOISS9	-2.052	1.974
	KOISS10	-1.752	1.463
	KOISS11	-2.364	1.420
	KOISS12	-2.032	1.798
	KOISS13	-2.143	1.850
Knowledge of Security Technology (KSTG)	KSTG1	-2.091	1.914
	KSTG2	-2.316	2.247
	KSTG3	-2.228	2.221
	KSTG4	-1.984	1.995
	KSTG5	-1.973	2.028
Knowledge of Legislation, Regulation and National Culture (KLRNC)	KLRNC1	-2.089	1.870
	KLRNC2	-2.135	1.863
	KLRNC3	-2.062	1.800
	KLRNC4	-1.832	1.812
	KLRNC5	-2.225	2.048
	KLRNC6	-1.966	1.876
	KLRNC7	-2.105	1.438
	KLRNC8	-2.129	1.911
	KLRNC9	-2.205	1.851
Knowledge of Security Responsibility (KSRS)	KSRS1	-2.399	1.847
	KSRS2	-2.339	1.672
	KSRS3	-2.226	1.709
	KSRS4	-2.543	2.059
	KSRS5	-2.326	1.980
	KSRS6	-2.357	2.001
	KSRS7	-2.322	2.039
	KSRS8	-2.413	1.905
	KSRS9	-2.378	1.615
	KSRK1	-2.238	1.698
	KSRK2	-2.225	1.863

Knowledge of Security Risk (KSRK)	KSRK3	-2.068	1.893
	KSRK4	-2.262	2.105
	KSRK5	-2.182	1.787
	KSRK6	-2.019	1.768
	KSRK7	-2.079	1.770
Behaviour (BH)	BH1	-2.106	2.314
	BH2	-2.056	2.330
	BH3	-2.436	2.423
	BH4	-2.701	2.642
	BH5	-2.796	2.360
	BH6	-2.619	2.403
	BH7	-2.600	2.340
	BH8	-2.504	2.317
	BH9	-2.726	2.353
	BH10	-2.324	2.436
	BH11	-2.470	2.470
	BH12	-2.411	2.256
	BH13	-3.858	1.042
	BH14	-3.743	0.994
	BH15	-2.270	2.413
Attitudes (AT)	AT1	-1.997	1.734
	AT2	-2.138	1.716
	AT3	-1.791	1.806
	AT4	-2.057	1.761
	AT5	-2.132	1.968
	AT6	-1.855	1.646
	AT7	-1.955	1.725

As shown in Table 6.1, the results indicate that the standardised (z) scores of the observations for the research variables take the range from -3.858 to 2.642, suggesting that none of the variable surpassed the threshold of ±4. Thus there is no uni-variate outliers among the observations.

6.2.2.2 Multivariate Outliers

The data were examined further by using multivariate detection. Mahalanobis distance works successfully in recognising multivariate outliers.

Mahalanobis D-squared distances are produced for each case using AMOS regression with case number being the dependent variable and all non-demographic measures functioning as the independent variables. High D^2 / df value more than **3.5** speaks for the potential multivariate outlier (Hair et al., 1998). As shown in Appendix F, the results highlighted that the largest D^2 value is 103.449 (belonging to case 250). With respect to the 148 exogenous and endogenous variables and their relative estimation errors in this study (Appendix E), the maximum D^2 / df was equal to 0.699 (103.449/ 148), far below the cut-off 3.5. Therefore, it can be concluded that the examination of D^2 values for all cases did not imply that there are multivariate outliers, which means that all observations had to be kept for analysis.

6.2.3 Assessment of Data Normality

The normality test was conducted to serve as the main pre-assumption of maximum likelihood estimation for the evaluation of the normal distribution of the data constructs. Table 6.2 shows the results of normality test for all items and variables used in the model.

Table 6.2 Assessment of Normality for Measurement Model

Construct	**Item**	**Skewness**	**Std. Error of Skewness**	**Kurtosis**	**Std. Error of Kurtosis**
Knowledge of Security Threat (KSTH)	KSTH1	-0.055	-0.427	-0.794	-3.081
	KSTH2	-0.064	-0.499	-0.523	-2.03
	KSTH3	-0.144	-1.115	-0.214	-0.828
	KSTH4	-0.3	-2.33	-0.311	-1.205
	KSTH5	-0.115	-0.895	-0.646	-2.505
Knowledge of Organisation Information Security Strategy (KOISS)	KOISS1	-0.064	-0.493	-0.72	-2.792
	KOISS2	-0.027	-0.211	-0.355	-1.376
	KOISS3	-0.298	-2.311	-0.762	-2.954
	KOISS4	0.101	0.783	-0.364	-1.413
	KOISS5	-0.146	-1.134	-0.494	-1.918
	KOISS6	0.071	0.55	-0.757	-2.935
	KOISS7	-0.148	-1.152	-0.478	-1.855
	KOISS8	0.044	0.344	-0.737	-2.859
	KOISS9	-0.146	-1.13	-0.598	-2.319
	KOISS10	-0.231	-1.794	-1.006	-3.901
	KOISS11	-0.759	-5.891	0.072	0.278
	KOISS12	0.18	1.398	-0.689	-2.672
	KOISS13	-0.214	-1.658	-0.556	-2.155
	KSTG1	-0.044	-0.341	-0.944	-3.662
	KSTG2	-0.034	-0.266	-0.168	-0.652

Knowledge of Security Technology (KSTG)	KSTG3	0.018	0.136	-0.378	-1.468
	KSTG4	-0.055	-0.423	-0.375	-1.453
	KSTG5	0.122	0.948	-0.648	-2.512
Knowledge of Legislation, Regulation and National Culture (KLRNC)	KLRNC1	-0.11	-0.851	-0.395	-1.532
	KLRNC2	0.026	0.202	-0.37	-1.436
	KLRNC3	-0.033	-0.257	-0.627	-2.43
	KLRNC4	-0.11	-0.855	-0.669	-2.594
	KLRNC5	0.099	0.766	-0.493	-1.913
	KLRNC6	0.039	0.303	-0.527	-2.046
	KLRNC7	-0.568	-4.406	-0.484	-1.877
	KLRNC8	-0.149	-1.152	-0.509	-1.976
	KLRNC9	-0.024	-0.184	-0.73	-2.83
Knowledge of Security Responsibility (KSRS)	KSRS1	-0.259	-2.012	-0.434	-1.685
	KSRS2	-0.13	-1.009	-0.698	-2.706
	KSRS3	-0.194	-1.505	-0.48	-1.864
	KSRS4	-0.42	-3.258	-0.138	-0.537
	KSRS5	-0.115	-0.895	-0.378	-1.467
	KSRS6	0.017	0.131	-0.281	-1.091
	KSRS7	-0.108	-0.841	-0.097	-0.375
	KSRS8	-0.252	-1.953	-0.486	-1.885
	KSRS9	-0.239	-1.856	-0.295	-1.145
Knowledge of Security Risk (KSRK)	KSRK1	-0.393	-3.05	-0.379	-1.47
	KSRK2	-0.325	-2.518	-0.349	-1.355
	KSRK3	-0.162	-1.255	-0.681	-2.642
	KSRK4	-0.143	-1.106	-0.082	-0.316
	KSRK5	-0.341	-2.648	-0.32	-1.242
	KSRK6	-0.04	-0.312	-0.766	-2.969
	KSRK7	-0.131	-1.016	-0.535	-2.075
Behaviour (BH)	BH1	0.434	3.366	-0.301	-1.166
	BH2	0.314	2.437	-0.407	-1.58
	BH3	-0.01	-0.079	0.081	0.312
	BH4	0.004	0.03	-0.046	-0.177
	BH5	0.128	0.989	0.191	0.742
	BH6	0.176	1.365	0.281	1.091
	BH7	0.372	2.888	-0.029	-0.113
	BH8	0.059	0.46	0.299	1.159
	BH9	0.111	0.864	0.38	1.473
	BH10	0.258	1.998	-0.33	-1.279
	BH11	0.126	0.976	-0.381	-1.479
	BH12	0.244	1.891	-0.499	-1.936
	BH13	-1.109	-8.601	1.649	6.397
	BH14	-1.253	-9.72	2.086	8.092
	BH15	0.277	2.15	-0.314	-1.219
Attitudes (AT)	AT1	-0.256	-1.985	-0.615	-2.384
	AT2	-0.252	-1.956	-0.499	-1.935

	AT3	0.114	0.881	-0.698	-2.707
	AT4	-0.255	-1.975	-0.662	-2.568
	AT5	-0.179	-1.389	-0.482	-1.871
	AT6	-0.167	-1.295	-0.728	-2.823
	AT7	-0.197	-1.525	-0.501	-1.944

As illustrated in table 6.2, the skew range is from -1.253 to 0.434 and the kurtosis range is from -1.006 to 2.086. The result shows that the skew and kurtosis of all items and variables are within the range of ±3 and ±7 respectively. Therefore, the data set of all items are concluded to be well-modelled by a normal distribution.

6.3 Sample Profile

Table 6.3 represents the frequencies and percentages of the demographic variables.

Table 6.3 Sample Profile

Group	Frequency	Percentage
Gender		
Male	176	48.8
Female	185	51.2
Age		
Above 45	44	12.2
36-45	97	26.9
25-35	136	37.7
25 under	84	23.3
Experience		
More than 10 year	103	28.5
5-10 Years	112	31.0
2-4 Years	74	20.5
Less than a year	72	19.9
Job Level		
Doctor	62	17.2
Hospital Management	47	13.0
Administartartive Staff	129	35.7
Nurse	123	34.1
Education		
Postgraduate	67	18.6
Undergraduate	294	81.4

IT Working		
NO	265	73.4
YES	96	26.6
IT Education		
NO	242	67.0
YES	119	33.0
Work Requirement		
NO	0	0
YES	361	100
Security Awareness Training		
NO	281	77.8
YES	80	22.2

Over 361 questionnaires that were gathered, 176 useful responses were received from the male respondents (48.8%) and 185 from female respondents (51.2%). Therefore, the sample of this study is equally represented by both genders.

The respondents were required to specify their age. Based on the result, 12.2% of the respondents stated that they were above 45 years old, 26.9% between 36 to 45 years old, 37.7% 25 to 35 years old and 23.3% stated that they were less than 25 years old.

Respondents were also asked to specify the number of years of working experience. 28.5% of the respondents stated that they have more than 10 years of work experience. 31.0% have 5 to 10 years of working experience, 20.5% have 2 to 4 years of working experience and 19.9% of the respondents have less than one year of working experience.

In specifying the job level of the respondents, 17.2% of them were Doctors, 13.0% were part of Hospital Management, 35.7% were Administrative Staff and 34.1% were Nurses.

The respondents were also asked to state their educational level. Based on the result, 18.6% of them have Postgraduate degree while 81.4% have Undergraduate degree.

The results also indicated that 26.6% of the respondents worked in IT department while 73.4% did not work in IT department.

33.0% of the respondents had education background in IT while 67.0% did not have.

100% of the respondents stated that their work require dealing with computer or IT technology and 22.2% stated that they had undergone security awareness training.

6.4 Measurement Model (CFA) – Stage 1 of SEM

The construct operationalization stands out as a very important step (Hair et al., 2006) to ensure accuracy. Researchers can choose from a number of established scales to try and ensure that there is theoretical accuracy. However, although there are existing scales available, Hair et al. (2006) admit that there is a lack of established scales and they are driven to work on new measurement scales or greatly modify the existing scales to cater for the new context. Upon these considerations, the basis of the SEM analysis lies in the selection of items that can measure the constructs (Hair et al., 2006).

In this study, 70 items were used to measure eight latent constructs namely: Knowledge of Security Threat (KSTH), Knowledge of Organisation Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS), Knowledge of Security Risk (KSRK), Behaviour (BH) and Attitudes (AT). The initial CFA model with all 70 items was portrayed in Appendix F.

6.4.1 Standardized Loadings of the Model's Items

Table 6.4 shows the deleted items from the model and the recalculated factor loadings for the remaining items.

Table 6.4 Initial Standardized Factor Loadings of the Items in CFA Model

Construct	**Item**	**Initial Factor Loading**	**Item Deleted**	**Second Factor Loading**
Knowledge of Security Threat (KSTH)	KSTH1	0.862		0.862
	KSTH2	0.783		0.783

	KSTH3	0.819		0.819
	KSTH4	0.788		0.788
	KSTH5	0.793		0.793
Knowledge of Organisation Information Security Strategy (KOISS)	KOISS1	0.793		0.797
	KOISS2	0.719		0.721
	KOISS3	0.735		0.739
	KOISS4	0.725		0.727
	KOISS5	0.801		0.8
	KOISS6	0.728		0.729
	KOISS7	0.735		0.741
	KOISS8	0.77		0.773
	KOISS9	0.793		0.792
	KOISS10	0.437	Deleted	
	KOISS11	0.298	Deleted	
	KOISS12	0.726		0.718
	KOISS13	0.694		0.696
Knowledge of Security Technology (KSTG)	KSTG1	0.803		0.803
	KSTG2	0.77		0.771
	KSTG3	0.783		0.783
	KSTG4	0.853		0.852
	KSTG5	0.762		0.762
Knowledge of Legislation, Regulation and National Culture (KLRNC)	KLRNC1	0.723		0.724
	KLRNC2	0.757		0.755
	KLRNC3	0.79		0.793
	KLRNC4	0.723		0.719
	KLRNC5	0.784		0.787
	KLRNC6	0.752		0.752
	KLRNC7	0.383	Deleted	
	KLRNC8	0.787		0.788
	KLRNC9	0.815		0.818
Knowledge of Security Responsibility (KSRS)	KSRS1	0.793		0.794
	KSRS2	0.774		0.774
	KSRS3	0.75		0.754
	KSRS4	0.76		0.762
	KSRS5	0.68		0.685
	KSRS6	0.781		0.778
	KSRS7	0.7		0.697
	KSRS8	0.666		0.671
	KSRS9	0.398	Deleted	
Knowledge of Security Risk (KSRK)	KSRK1	0.805		0.805
	KSRK2	0.687		0.687
	KSRK3	0.688		0.688
	KSRK4	0.79		0.79
	KSRK5	0.752		0.752
	KSRK6	0.72		0.72

	KSRK7	0.808		0.808
Behaviour (BH)	BH1	0.768		0.768
	BH2	0.759		0.759
	BH3	0.734		0.734
	BH4	0.697		0.697
	BH5	0.744		0.744
	BH6	0.736		0.736
	BH7	0.745		0.745
	BH8	0.769		0.769
	BH9	0.732		0.732
	BH10	0.774		0.774
	BH11	0.768		0.768
	BH12	0.748		0.748
	BH13	-0.002	Deleted	
	BH14	0.028	Deleted	
	BH15	0.798		0.798
Attitudes (AT)	AT1	0.714		0.714
	AT2	0.725		0.724
	AT3	0.732		0.732
	AT4	0.759		0.759
	AT5	0.726		0.726
	AT6	0.788		0.788
	AT7	0.75		0.75

As shown in Table 6.4, the results derived from the evaluation of the standardized loadings of the model's items illustrated that the factor loadings of KOISS10, KOISS11, KLRNC7, KSRS9, BH13 and BH14 were 0.437, 0.298, 0.383, 0.398, -0.002 and 0.028 respectively. All of these values are not more than cut-off value of 0.5. Therefore, these six items were taken out from the model. The revised model with 64 remaining items was tested again to check whether or not the factor structure could stay stable. In effect, the second standardised factor loadings for all items were more than 0.5, which is from 0.671 to 0.862 (See Appendix G). Therefore, no further item was deleted because otherwise the factor loading will not be sufficient.

6.4.2 Goodness of Fit Indices

The results indicated that even after the removal, the second iteration of the measurement model still give poor fit for the data with the remaining 64 items (Appendix G). The GFI was 0.796, which is below the cut-off value of 0.8 as put forth by Fornell & Larcker (1981), Hair et al. (2006) and Kline (2005). The AGFI was 0.779, below the cut-off value of 0.8 as proposed by Chau & Hu (2001). Thus the model was improved by looking at the modification indices and standardised residual covariance of each item.

The model indicated that some of items showed high discrepancy of covariance between their related errors (M.I. above 15), indicating the presence of redundant items in the model. For instance, the M.I value of covariance between the errors of AT1 and AT3 was 33.024. It means, if the analysis is repeated, treating the covariance between the error of these two items as a free parameter, the discrepancy will fall by at least 33.024. Both items loaded on a same construct (i.e Attitude). Thus the covariance between their errors refers to within-construct error covariance. The other within-construct error covariance was located between KSRK6 and KSRK7. The within-construct error covariance terms are threats to construct validity (DeVellis, 2016). Drawing correlation paths between these errors and allowing these paths to be estimated (freeing them) will reduce the χ^2 and improve the model fit (Rutherford, Hair, Anderson & Tatham, 1988). Therefore, the decision of modifying the model was to draw correlation paths between these items' errors.

Also, the model indicated covariance between the error terms of indicator variables loading on various constructs. At this point, the high M.I covariance values of the errors of BH1, BH6 and KSRS1 with the items' errors of other constructs refer to between-construct error covariance. The significance between-construct error covariance suggests that the items that have to do with this error term have more association with one another than the original measurement model would forecast. Such phenomenon implies that there is a significant cross-loading that exists in the model which can bring about poor discriminant validity (Bentler, 1980). Thus, the decision to modify the model was to reduce these three items from the model rather than drawing correlation path between the items' errors (Awang, 2012).

The examination of standardized residual covariance indicated that the absolute values of KOISS12, KSTG5, BH5, AT7 and BH10 were higher than the threshold value of 2.58 with other items in the model. Therefore it was decided that these five items were to be removed from the model. The results indicated that the remaining items have an acceptable absolute value lower than the threshold 2.58 with other items in the model.

After removing these items iteratively, the overall measurement model that has the 56 remaining items was performed once again in Figure 6.1. The results of the goodness of fit indices of the measurement model are presented in Table 6.5.

Table 6.5 GOF Indices of Modified Measurement Model

Fit index	**Modified Model**	**Recommended Values**	**Acceptable Values**	**Source**
Df	1453			
CMIN (χ^2)	2077.908			
p-value	0.000	> 0.05	≥ 0.000	Hair Jr, Anderson, Tatham, & William, 1998; Joreskog & Sorbom,
χ^2/df	1.430	≤ 3.00	≤ 5.00	Bagozzi & Yi (1988)
GFI	0.836	≥ 0.90	≥ 0.80	Fornell & Larcker (1981), Hair et al. (2006) ; Kline (2010)
AGFI	0.819	≥ 0.80	≥ 0.80	Chau & Hu (2001)
CFI	0.946	≥ 0.90	≥ 0.90	Bagozzi and Yi (1988); Byrne, 2013
TLI	0.945	≥ 0.90	≥ 0.90	Hair et al., (2006); Ho, (2006)
IFI	0.949	≥ 0.90	≥ 0.90	Hair et al., (2006); Ho, (2006)
RMSEA	0.035	0.05 to 0.08	≤ 0.10	Schumacker & Lomax, 2010

The results have given the indication that the modified overall measurement model gave an adequate fit of the data with all the remaining 56 items where Chi-square = 2077.908, df = 1453, p-value = 0.000. The results of the GOF established that the chi-square was significant at 0.001 level. Nevertheless, the absolute fit index of minimum discrepancy chi-square can be dismissed if the sample size obtained for the study is larger than 200 (Hair et al., 1998; Jöreskog & Sörbom, 2010). The value of GFI was 0.836, which is less than the recommended value of 0.9, but it is still was at a marginal acceptance level and relatively close to the preferred value. Fornell & Larcker (1981) argued that value of GFI less than 0.9 does not necessarily mean that the model has a poor fit. Hair et al. (2006) & Kline (2015) stated that the GFI values between 0.8 and 0.9 are still within the acceptable fit. After the adjustment for the degrees of freedom relative to the number of variables, the adjusted GFI (AGFI) was 0.819 which was above the cut-off point of 0.80 as recommended by (Chau & Hu, 2001). One indication is that the model predicts 82% of the variances and covariance in the survey data. With the basis on the CFI, TLI, and IFI indices with values more than the cut off value of 0.9 (0.946, 0.945 and 0.949 respectively), the model had a credible fit of data (Bargozzi & Yi, 1988; Byrne, 2013; Hair et al., 2006). Furthermore, the root-mean-square error of approximation (RMSEA) was 0.035 which was not above the threshold value of 0.1 as suggested by (Schumacker & Lomax, 2004). Furthermore, the Relative CMIN/df was 1.430 which is not more than 5, demonstrating the good fit of the model (Bargozzi & Yi, 1988). Given that the measurement model fits the data in an adequate manner, no adjustment would be necessary.

6.4.3 Reliability and Convergent Validity

When the uni-dimensionality of the constructs was reached, each construct was evaluated for its reliability and validity. The assessment of the reliability was carried out using Cronbach's alpha, composite reliability (CR) and average variance extracted (AVE), whilst for validity, the construct, including convergent and discriminant were used. Table 6.6 represents the result of Cronbach alpha and convergent validity for the second iterative CFA model with 56 remaining items.

Table 6.6 Results of Cronbach Alpha and Convergent Validity for Measurement Model

Construct	**Item**	**Final Factor Loading**	**Average Variance Extracted (AVE)**^{a}	**Composite Reliability (CR)**^{b}	**Internal Reliability Cronbach Alpha**
Knowledge of Security Threat (KSTH)	KSTH1	0.862	0.655	0.905	0.904
	KSTH2	0.783			
	KSTH3	0.82			
	KSTH4	0.787			
	KSTH5	0.793			
Knowledge of Organisation	KOISS1	0.794	0.567	0.929	0.929
	KOISS2	0.719			
	KOISS3	0.748			

Information Security Strategy (KOISS)	KOISS4	0.733			
	KOISS5	0.794			
	KOISS6	0.719			
	KOISS7	0.745			
	KOISS8	0.778			
	KOISS9	0.795			
	~~KOISS10~~	0.437[c]			
	~~KOISS11~~	0.298[c]			
	~~KOISS12~~	0.718[e]			
	KOISS13	0.695			
Knowledge of Security Technology (KSTG)	KSTG1	0.807	0.640	0.877	0.876
	KSTG2	0.757			
	KSTG3	0.783			
	KSTG4	0.851			
	~~KSTG5~~	0.762 [e]			
Knowledge of Legislation, Regulation and National Culture (KLRNC)	KLRNC1	0.724	0.590	0.920	0.919
	KLRNC2	0.754			
	KLRNC3	0.793			
	KLRNC4	0.719			
	KLRNC5	0.787			
	KLRNC6	0.752			
	~~KLRNC7~~	0.383[c]			
	KLRNC8	0.789			
	KLRNC9	0.819			
Knowledge of Security Responsibility (KSRS)	~~KSRS1~~	0.794 [d]	0.539	0.891	0.890
	KSRS2	0.781			
	KSRS3	0.776			
	KSRS4	0.747			
	KSRS5	0.671			
	KSRS6	0.75			
	KSRS7	0.716			
	KSRS8	0.689			
	~~KSRS9~~	0.398[c]			
Knowledge of Security Risk (KSRK)	KSRK1	0.797	0.571	0.903	0.900
	KSRK2	0.686			
	KSRK3	0.687			
	KSRK4	0.783			
	KSRK5	0.743			
	KSRK6	0.751			
	KSRK7	0.831			
Behaviour (BH)	~~BH1~~	0.768[d]	0.569	0.922	0.921
	BH2	0.763			
	BH3	0.731			
	BH4	0.695			
	~~BH5~~	0.744 [e]			

	~~BH6~~	0.736[d]			
	BH7	0.747			
	BH8	0.779			
	BH9	0.745			
	~~BH10~~	0.774[e]			
	BH11	0.76			
	BH12	0.76			
	~~BH13~~	-0.002[c]			
	~~BH14~~	0.028[c]			
	BH15	0.803			
Attitudes (AT)	AT1	0.74	0.560	0.884	0.879
	AT2	0.723			
	AT3	0.75			
	AT4	0.736			
	AT5	0.728			
	AT6	0.811			
	~~AT7~~	0.75[e]			

a: Average Variance Extracted = (summation of the square of the factor loadings)/{(summation of the square of the factor loadings) + (summation of the error variances)}.
b: Composite reliability = (square of the summation of the factor loadings)/{(square of the summation of the factor loadings) + (square of the summation of the error variances)}.
c: denotes for discarded item due to insufficient factor loading below cut off 0.5.
d: denotes for discarded item due to high between-construct error covariance above threshold 15
e: denotes for discarded item due to high standardized residual covariance above threshold 2.58

The number of deleted items (14 deleted items) was relatively high compared to the total items in the constructs (70 items). Nevertheless, their removal does not significantly change the content of the constructs as they are conceptualized. As shown in Table 6.6, the remaining indicators have high factor loadings ranging from 0.671 to 0.862 indicating that the meaning of the factors has been preserved by these indicators.

Table 6.6 also illustrates that the AVE, which reflects the overall amount of variance in the indicators accounted for by the latent construct, are 0.655, 0.567, 0.640, 0.590, 0.539, 0.571, 0.569 and 0.560 for Knowledge of Security Threat (KSTH), Knowledge of Organisation Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS), Knowledge of Security Risk (KSRK), Behaviour (BH) and Attitudes (AT) respectively. As proposed by Nunnally & Bernstein (1994), all these values were higher than the cut-off value of 0.5 .

The composite reliability values that represent the degree of indication of the latent construct given by the construct indicators are 0.905, 0.929, 0.877, 0.920, 0.891, 0.903, 0.922 and 0.884 for Knowledge of Security Threat (KSTH), Knowledge of Organisation Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS), Knowledge of Security Risk (KSRK), Behaviour (BH) and Attitudes (AT) respectively. All these values exceeded the recommended value of 0.6 as recommended by Bargozzi & Yi (1988).

The Cronbach's Alpha value, that sheds light on the degree to which a measure is free from errors are 0.904, 0.929, 0.876, 0.919, 0.890, 0.900, 0.921 and 0.879 for Knowledge of Security Threat (KSTH), Knowledge of Organisation Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS), Knowledge of Security Risk (KSRK), Behaviour (BH) and Attitudes (AT) respectively. All these values were higher than the threshold value of 0.7 as suggested by Nunnally & Bernstein (1994). Therefore, the Cronbach's Alpha achieved for all constructs was deemed to be sufficiently error-free.

6.4.4 Discriminant validity

The Discriminant validity was studied to assess how distinct a construct is from other constructs. As for the discriminant validity, the correlations between factors in the measurement model do not exceed 0.85 as mentioned by (Kline, 2005). The validity was checked depending on the comparisons drawn between constructs and square root of the average variance extracted for a construct (Fornell & Larcker, 1981). Table 6.7 depicts the discriminant validity of the measurement model.

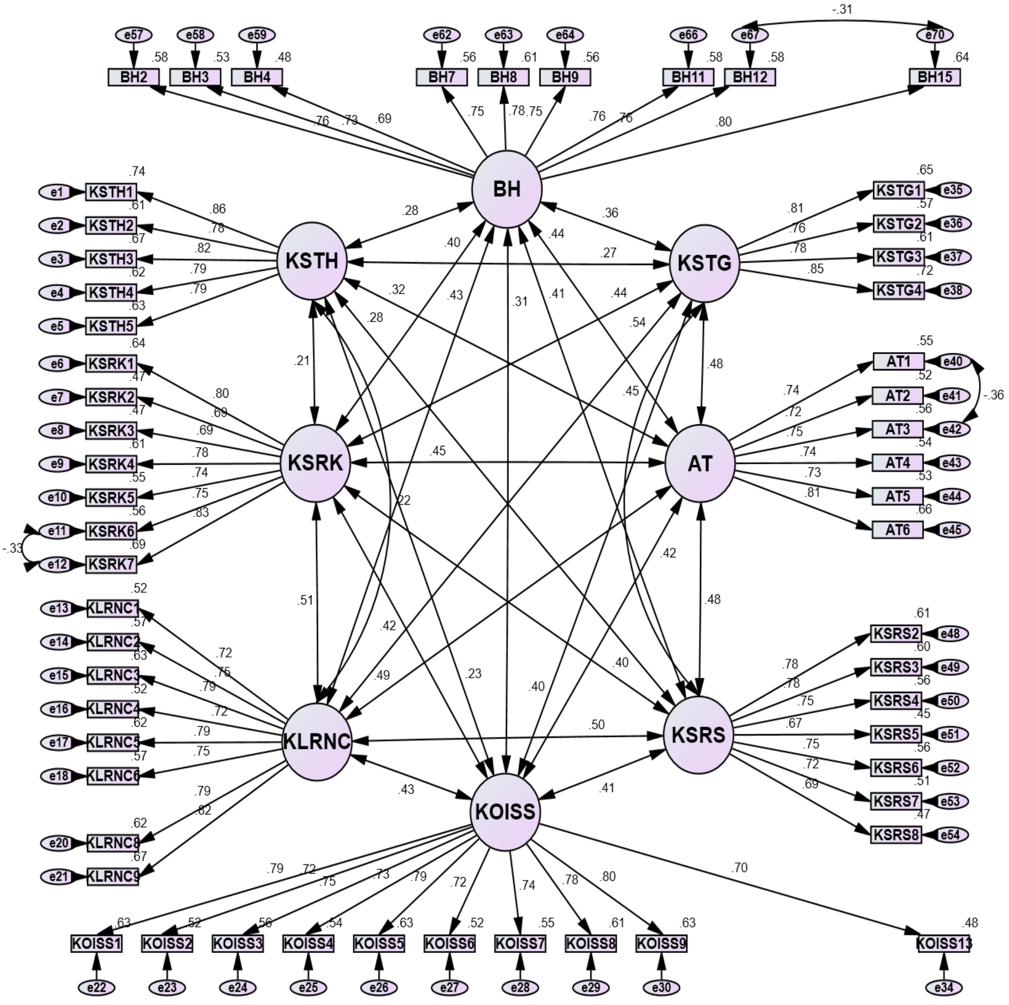
Table 6.7 Discriminant validity for Measurement Model

	KSTG	KSTH	AT	BH	KOISS	KSRK	KLRNC	KSRS
KSTG	**0.800**							

KSTH	0.266	**0.810**						
AT	0.479	0.325	**0.749**					
BH	0.361	0.277	0.437	**0.754**				
KOISS	0.398	0.234	0.424	0.312	**0.753**			
KSRK	0.438	0.209	0.446	0.400	0.417	**0.756**		
KLRNC	0.541	0.218	0.486	0.426	0.427	0.505	**0.768**	
KSRS	0.454	0.283	0.477	0.411	0.407	0.396	0.496	**0.734**

Note: Diagonals represent the square root of the average variance extracted while the other entries represent the square correlations.

The inter-correlations between the six constructs had a range from 0.209 to 0.541, or below the threshold 0.85 as recommended by (Kline, 2005). Also, as shown in Table 6.7, the correlations were not more than the square root of the average variance extracted by the indicators, and this suggests that there is a good discriminant validity between these factors (Kline, 2005). To determine the goodness to fit of data, convergent validity and discriminant validity of the measurement model, in sum, the modified measurement scale to assess the constructs and their relative items was found to be reliable and valid. Figure 6.1 depicts the measurement model with standardized factor loadings for the remaining 56 items.



Absolute Fit Indices
df = 1453
Chi Square = 2077.908

p-value = .000
GFI = .836
AGFI = .819
RMSEA = .035

Incremental Fit Indices
CFI = .948
TLI = .945
IFI = .949

Parsimonious Fit Index
NORMEDCHISQ = 1.430

Figure 6.1 Measurement Model with Remaining 56 Items

6.5 Descriptive Analysis

In this analysis, covariance matrix method was performed to calculate the descriptive function so that all of the variables could also be part of the analysis. The composite scores of the variables were computed by parcelling the scores of the original measurement item. Parcels are sum or averages of several individual indicators or items with regard to their factor loadings on the construct (Coffman & MacCallum, 2005; Hair et al., 2006). Table 6.8 shows the mean and standard deviation of the constructs, evaluated on a 5-point Likert scale:

Table 6.8 Results of Descriptive Statistic for Variables

Constructs	Mean	Standard Deviation	Minimum	Maximum
Knowledge of Security Threat (KSTH)	3.178	0.819	1.4	4.8
Knowledge of Organisation Information Security Strategy (KOISS)	3.103	0.801	1.4	4.6
Knowledge of Security Technology (KSTG)	3.018	0.804	1.4	4.8
Knowledge of Legislation, Regulation and National Culture (KLRNC)	3.116	0.808	1.4	4.6
Knowledge of Security Responsibility (KSRS)	3.232	0.727	1.4	4.6
Knowledge of Security Risk (KSRK)	3.157	0.794	1.1	4.7
Behaviour (BH)	3.025	0.642	1.5	4.7
Attitudes (AT)	3.116	0.832	1.4	4.4

As a measure of central tendency, the mean was applied, and this indicated that the mean values of all constructs were higher than their midpoint level (3) as indicated in table 6.8. The phenomenon indicated that the consensus respondents' perception toward these constructs were higher than the average. The highest mean rating belonged to Knowledge of Security Responsibility (KSRS) with the mean value 3.227. The lowest mean rating was attached to Behaviour (BH) with the mean value of 3.024.

The standard deviation was applied as a dispersion index to show the degree to which individuals within each variable are dissimilar to the variable mean. Among the variables focused, the individual value of Attitudes (AT) strayed from its mean (SD = 0.830). This standard deviation suggested high variability in respondents' perception toward Attitudes (AT). Put simply, the survey participants were most varying in this variable from each other. Conversely, the lowest deviation from mean belonged to Behaviour (BH) with the standard deviation noted to be 0.640. Figure 6.2 provides a good illustration for the mean of all variables and their standard deviations.

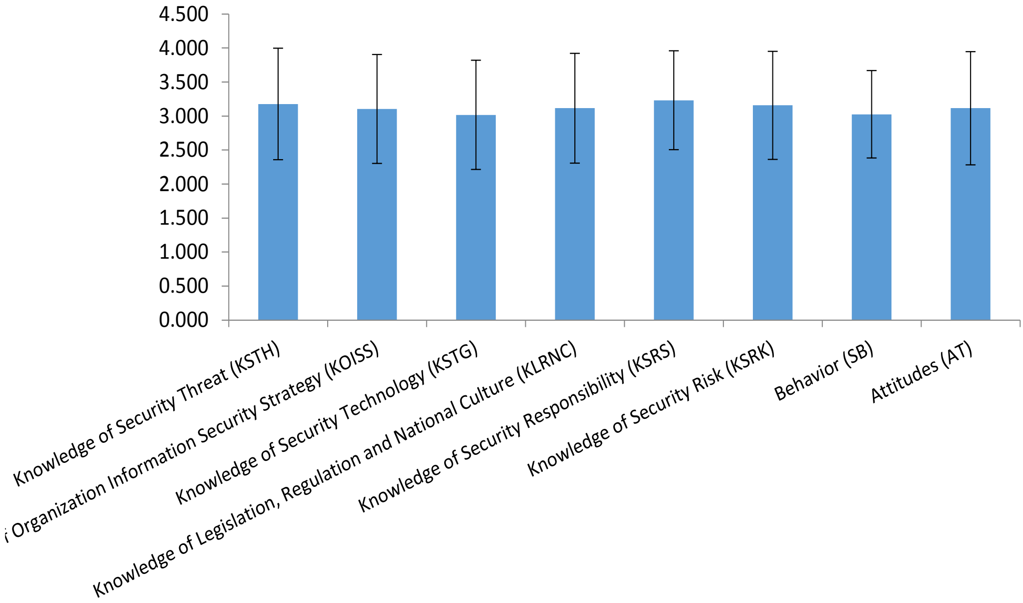


Figure 6.2 Means and Standard Variations of All Variables

6.6 Structural Models - Stage 2 of SEM

The structural equation model is the second main process carried out in the SEM analysis. Once the measurement model is validated, the structural model represented can be made by specifying the relationships of the constructs. The structural model gives details on the links between the variables. It demonstrates the particular details of the relationship between the independent or exogenous variables and dependent or endogenous variables (Hair et al., 2006 & Ho, 2006). The structural model evaluation has its main focus resting on the overall model fit, followed by the size, direction and significance of the hypothesized parameter estimates, as shown by the one-headed arrows in the path diagrams (Hair et al., 2006).

The final part entailed the confirmation of the structural model of the study based on the proposed relationship between the variables that were identified and assessed.

In this study the structural model was estimated to examine the research hypothesis, using AMOS and maximum likelihood estimate (MLE) technique.

The next sub-sections explain the details the development of structural model to examine the research hypotheses.

6.6.1 Direct Effects of Constructs

In the structural model, the direct effects of Knowledge of Security Threat (KSTH), Knowledge of Organisation Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) as independent variables on Attitudes (AT) and Behaviour (BH) as dependent variables were examined (i.e., H1.a, H2.a, H3.a, H4.a, H5.a, H6.a, H1.b, H2.b, H3.b, H4.b, H5.b, and H6.b respectively). The model also examined the direct effect of Attitudes (AT) on Behaviour (BH) (i.e., H7).

The AMOS graph of structural model for direct effects of the constructs together the standardized regression weights is portrayed in Figure 6.3.

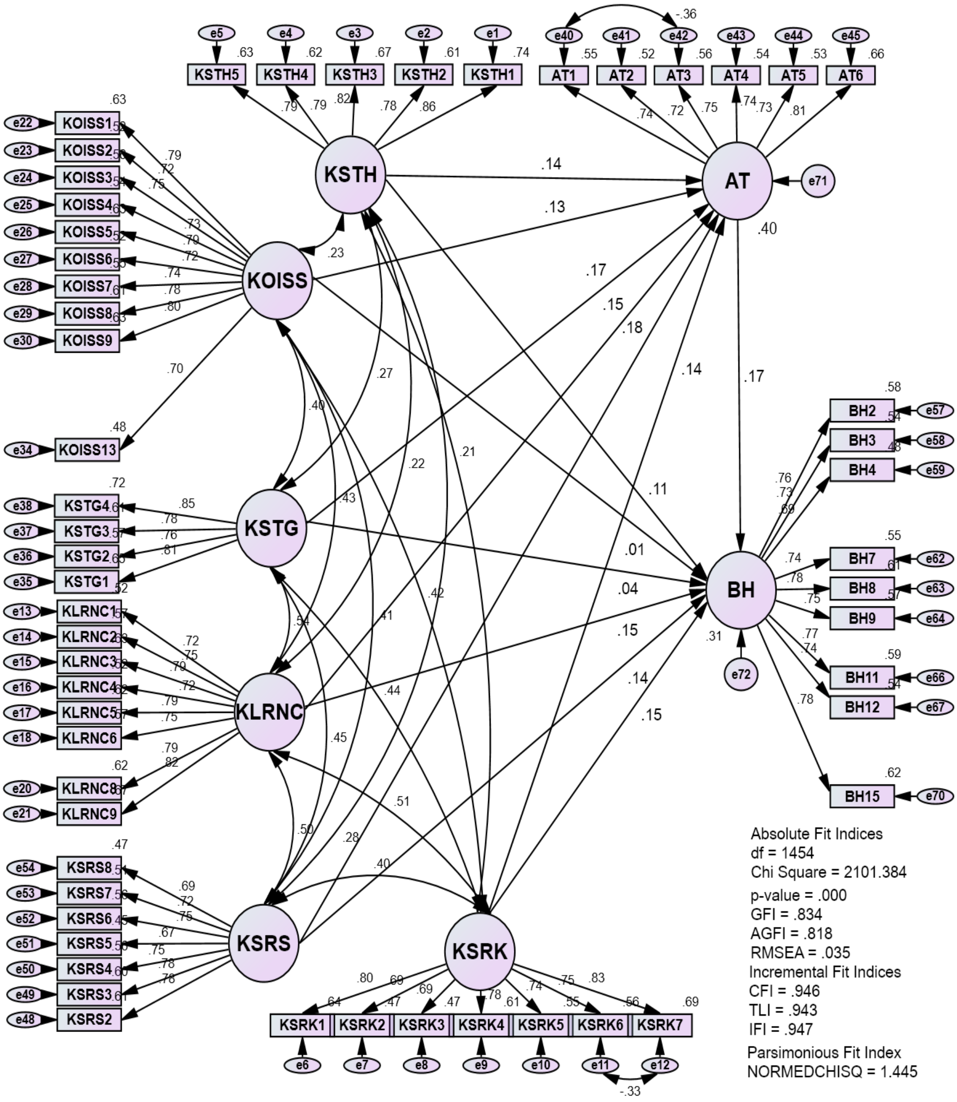


Figure 6.3 AMOS Graph of Structural Model

An examination of goodness-of-fit indices indicates that the structural model adequately fitted the data: χ^2 = 2101.384, df = 1454, p-value = 0.000, GFI = 0.834, AGFI = 0.818, CFI = 0.946, TLI = 0.943, IFI = 0.947, RMSEA =0.035 and χ^2/df= 1.445.

The value of R^2 for Attitudes (AT) and Behaviour (BH) was 0.40 and 0.31 respectively. This indicates, for example, the error variance of Behaviour (BH) is approximately 69 percent of the variance of Behaviour (BH) itself. In other word, 31 percent of variations in Behaviour (BH) are explained by its seven predictors (i.e., KSTH, KOISS, KSTG, KLRNC, KSRS, KSRK and AT). Overall findings showed that the score of R^2 value satisfy the requirement for the 0.30 cut off value (Quaddus & Hofmeyer, 2007).

The coefficient parameters estimates are then examined to test the hypothesized direct effects of the variables. The path coefficients and the results of examining hypothesized direct effects are displayed in Table 6.9.

Table 6.9 Examining Results of Hypothesized Direct Effects of the Constructs

Path	**Unstandardized Estimate**		**Standardised Estimate**	**critical ration (c.r.)**	**P-value**	**Hypothesis Result**
	Estimate	**S.E.**	**Beta**			
KSTH → AT	0.142	0.053	0.137^{**}	2.697	0.007	H1.a) Supported
KOISS → AT	0.142	0.063	0.129^{*}	2.268	0.023	H2.a) Supported
KSTG → AT	0.19	0.074	0.165^{*}	2.572	0.01	H3.a) Supported
KLRNC → AT	0.19	0.084	0.150^{*}	2.272	0.023	H4.a) Supported
KSRS → AT	0.241	0.083	0.179^{**}	2.899	0.004	H5.a) Supported
KSRK → AT	0.165	0.068	0.145^{*}	2.424	0.015	H6.a) Supported
KSTH → BH	0.082	0.039	0.114^{*}	2.112	0.035	H1.b) Supported
KOISS → BH	0.01	0.046	0.013	0.217	0.828	H2.b)Not Supported

KSTG → BH	0.031	0.054	0.039	0.576	0.565	H3.b)Not Supported
KLRNC → BH	0.129	0.062	0.146*	2.099	0.036	H4.b) Supported
KSRS → BH	0.136	0.062	0.144*	2.211	0.027	H5.b) Supported
KSRK → BH	0.121	0.05	0.151*	2.405	0.016	H6.b) Supported
AT → BH	0.122	0.047	0.174*	2.593	0.01	H7) Supported

*p< 0.05 , **p< 0.01, ***p< 0.001

As shown in table 6.9, six paths from Knowledge of Security Threat (KSTH), Knowledge of Organisation Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) on Attitudes (AT) as well as five paths from Knowledge of Security Threat (KSTH), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) and Attitudes (AT) on Behaviour (BH) were positively significant as their p-values were all below the standard significance level of 0.05. Thus the hypotheses H1.a, H2.a, H3.a, H4.a, H5.a, H6.a, H1.b, H4.b, H5.b, H6.b and H7 were supported. The following section discusses the results of path analysis in relation to the above hypotheses in the structural model:

H1.a) Knowledge of Security Threat (KSTH) has significant effect on Attitudes (AT)

As shown in table 6.9, the critical ration (c.r) and p-value of Knowledge of Security Threat (KSTH) in predicting Attitudes (AT) were 2.697 and 0.007 respectively. It means that the probability of getting a critical ratio as large as 2.697 in absolute value is 0.007. In other words, the regression weight for Knowledge of Security Threat (KSTH) in the prediction of Attitudes (AT) is significantly different from zero at the 0.01 level (two-tailed). Thus, H1.a was supported. Further, the standardized estimate of Beta was 0.137, indicating a positive relationship. It means, when Knowledge of Security Threat (KSTH) goes up by 1 standard deviation, Attitudes (AT) goes up by 0.137 standard deviations.

H2.a) Knowledge of Organisation Information Security Strategy (KOISS) has significant effect on Attitudes (AT)

The critical ration (c.r) and p-value of Knowledge of Organisation Information Security Strategy (KOISS) in predicting Attitudes (AT) were 2.268 and 0.023 respectively. It means that the probability of getting a critical ratio as large as 2.268 in absolute value is 0.023. In other words, the regression weight for Knowledge of Organisation Information Security Strategy (KOISS) in the prediction of Attitudes (AT) is significantly different from zero at the 0.05 level (two-tailed). Thus, H2.a was supported. Furthermore, the standardized estimate of Beta was 0.129, indicating a positive relationship. This mean that, when Knowledge of Organisation Information Security Strategy (KOISS) goes up by 1 standard deviation, Attitudes (AT) goes up by 0.129 standard deviations.

H3.a) Knowledge of Security Technology (KSTG) has significant effect on Attitudes (AT)

The critical ration (c.r) and p-value of Knowledge of Security Technology (KSTG) in predicting Attitudes (AT) were 2.527 and 0.01 respectively. It means that the probability of getting a critical ratio as large as 2.527 in absolute value is 0.01. In other words, the regression weight for Knowledge of Security Technology (KSTG) in the prediction of Attitudes (AT) is significantly different from zero at the 0.05 level (two-tailed). Thus, H3.a was supported. Furthermore, the standardized estimate of Beta was 0.165, indicating a positive relationship. This mean that when Knowledge of Security Technology (KSTG) goes up by 1 standard deviation, Attitudes (AT) goes up by 0.165 standard deviations.

H4.a) Knowledge of Legislation, Regulation and National Culture (KLRNC) has significant effect on Attitudes (AT)

The critical ration (c.r) and p-value of Knowledge of Legislation, Regulation and National Culture (KLRNC) in predicting Attitudes (AT) were 2.272 and 0.023 respectively. It means that the probability of getting a critical ratio as large as 2.272 in absolute value is 0.023. In other words, the regression weight for Knowledge of Legislation, Regulation and National

Culture (KLRNC) in the prediction of Attitudes (AT) is significantly different from zero at the 0.05 level (two-tailed). Thus, H4.a was supported. Furthermore, the standardized estimate of Beta was 0.150, indicating a positive relationship. This means that when Knowledge of Legislation, Regulation and National Culture (KLRNC) goes up by 1 standard deviation, Attitudes (AT) goes up by 0.150 standard deviations.

H5.a) Knowledge of Security Responsibility (KSRS) has significant effect on Attitudes (AT)

The critical ration (c.r) and p-value of Knowledge of Security Responsibility (KSRS) in predicting Attitudes (AT) were 2.899 and 0.004 respectively. It means that the probability of getting a critical ratio as large as 2.899 in absolute value is 0.004. In other words, the regression weight for Knowledge of Security Responsibility (KSRS) in the prediction of Attitudes (AT) is significantly different from zero at the 0.01 level (two-tailed). Thus, H5.a was supported. Furthermore, the standardized estimate of Beta was 0.179, indicating a positive relationship. This means that when Knowledge of Security Responsibility (KSRS) goes up by 1 standard deviation, Attitudes (AT) goes up by 0.179 standard deviations.

H6.a) Knowledge of Security Risk (KSRK) has significant effect on Attitudes (AT)

The critical ration (c.r) and p-value of Knowledge of Security Risk (KSRK) in predicting Attitudes (AT) were 2.424 and 0.015 respectively. It means that the probability of getting a critical ratio as large as 2.424 in absolute value is 0.015. In other words, the regression weight for Knowledge of Security Risk (KSRK) in the prediction of Attitudes (AT) is significantly different from zero at the 0.05 level (two-tailed). Thus, H6.a was supported. Furthermore, the standardized estimate of Beta was 0.145, indicating a positive relationship. This means that when Knowledge of Security Risk (KSRK) goes up by 1 standard deviation, Attitudes (AT) goes up by 0.145 standard deviations.

H1.b) Knowledge of Security Threat (KSTH) has significant effect on Behaviour (BH)

As shown in table 6.9, the critical ration (c.r) and p-value of Knowledge of Security Threat (KSTH) in predicting Behaviour (BH) were 2.112 and 0.035 respectively. It means that the probability of getting a critical ratio as large as 2.112 in absolute value is 0.035. In other words, the regression weight for Knowledge of Security Threat (KSTH) in the prediction of Behaviour (BH) is significantly different from zero at the 0.05 level (two-tailed). Thus, H1.b was supported. Furthermore, the standardized estimate of Beta was 0.114, indicating a positive relationship. This means that when Knowledge of Security Threat (KSTH) goes up by 1 standard deviation, Behaviour (BH) goes up by 0.114 standard deviations.

H2.b) Knowledge of Organisation Information Security Strategy (KOISS) has significant effect on Behaviour (BH)

As shown in table 6.9, the results showed no significant relationship between the Organisation Information Security Strategy (KOISS) and Behaviour (BH); β = 0.013, C.R. = 0.217, p= 0.828. Thus, H2.b was rejected.

H3.b) Knowledge of Security Technology (KSTG) has significant effect on Behaviour (BH)

The results showed no significant relationship between the Knowledge of Security Technology (KSTG) and Behaviour (BH); β = 0.039, C.R. = 0.576, p= 0.565. Thus, H3.b was rejected.

H4.b) Knowledge of Legislation, Regulation and National Culture (KLRNC) has significant effect on Behaviour (BH)

The critical ration (c.r) and p-value of Knowledge of Legislation, Regulation and National Culture (KLRNC) in predicting Behaviour (BH) were 2.099 and 0.036 respectively. It means that the probability of getting a critical ratio as large as 2.099 in absolute value is 0.036. In other words, the regression weight for Knowledge of Legislation, Regulation and National Culture (KLRNC) in the prediction of Behaviour (BH) is significantly different from zero at the 0.05 level (two-tailed). Thus, H4.b was supported. Furthermore, the standardized estimate of Beta was 0.146, indicating a positive relationship. This means that when Knowledge of Legislation, Regulation and National Culture (KLRNC) goes up by 1 standard deviation, Behaviour (BH) goes up by 0.146 standard deviations.

H5.b) Knowledge of Security Responsibility (KSRS) has significant effect on Behaviour (BH)

The critical ration (c.r) and p-value of Knowledge of Security Responsibility (KSRS) in predicting Behaviour (BH) were 2.211 and 0.027 respectively. It means that the probability of getting a critical ratio as large as 2.211 in absolute value is 0.027. In other words, the regression weight for Knowledge of Security Responsibility (KSRS) in the prediction of Behaviour (BH) is significantly different from zero at the 0.05 level (two-tailed). Thus, H5.b was supported. Furthermore, the standardized estimate of Beta was 0.144, indicating a positive relationship. This means that when Knowledge of Security Responsibility (KSRS) goes up by 1 standard deviation, Behaviour (BH) goes up by 0.144 standard deviations.

H6.b) Knowledge of Security Risk (KSRK) has significant effect on Behaviour (BH)

The critical ration (c.r) and p-value of Knowledge of Security Risk (KSRK) in predicting Behaviour (BH) were 2.405 and 0.016 respectively. It means that the probability of getting a critical ratio as large as 2.405 in absolute value is 0.016. In other words, the regression weight for Knowledge of Security Risk (KSRK) in the prediction of Behaviour (BH) is significantly different from zero at the 0.05 level (two-tailed). Thus, H6.b was supported. Furthermore, the standardized estimate of Beta was 0.151, indicating a positive relationship. This means that when Knowledge of Security Risk (KSRK) goes up by 1 standard deviation, Behaviour (BH) goes up by 0.151 standard deviations.

H7) Attitudes (AT) has significant effect on Behaviour (BH)

The critical ration (c.r) and p-value of Attitudes (AT) in predicting Behaviour (BH) were 2.593 and 0.01 respectively. It means that the probability of getting a critical ratio as large as 2.593 in absolute value is 0.01. In other words, the regression weight for Attitudes (AT) in the prediction of Behaviour (BH) is significantly different from zero at the 0.05 level (two-tailed). Thus, H7 was supported. Furthermore, the standardized estimate of Beta was 0.174, indicating a positive relationship. This means that, when Attitudes (AT) goes up by 1 standard deviation, Behaviour (BH) goes up by 0.174 standard deviations.

6.6.2 Mediation Effects of Attitudes (AT)

The mediation analysis was used to determine the mediation effects of Attitudes (AT) as mediating variable on the effects of Knowledge of Security Threat (KSTH), Knowledge of Organisation Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) as independent variables on Behaviour (BH) as the dependent variable (i.e., H1.c, H2.c, H3.c, H4.c, H5.c and H6.c respectively). Furthermore, the indirect effects of the independent variables on the dependent variable through the mediating variable were also examined.

The statistics behind mediation are correlation. Mathieu & Taylor (2006) suggested a decision tree framework to test the covariance relationships among three variables: an independent variable (IV), a potential mediating variable (M) and a dependent variable (DV). The illustration of this framework.is shown in Figure 6.4.

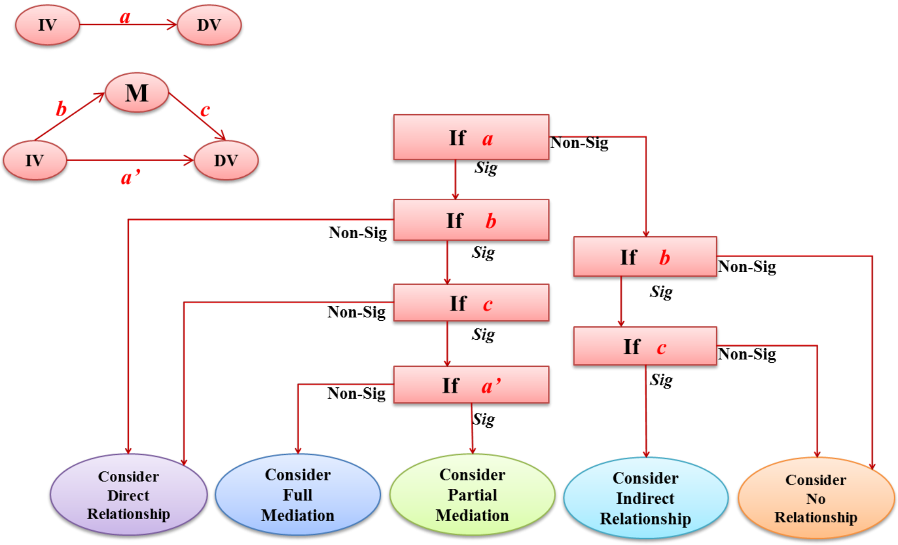


Figure 6.4 Decision tree for evidence supporting different intervening effects (Source: Mathieu & Taylor, 2006)

Based on this framework, the most important precondition that must be met to find significant mediation is that all three correlations among the three variables (paths a, b & c) must be statistically significant. If even one of these three correlations is not significant, then there would be no possibility to find significant mediation (Baron & Kenny, 1986; Mathieu & Taylor, 2006). Upon significant relations among the three variables (paths a, b & c), once the direct effect of IV on DV in the multiple regression (path a') is not statistically significant, then the mediating variable act as a full mediator. Otherwise, the mediation can be considered as partial mediation. In the absence of full or partial mediation, the relationships between IV and DV can either be direct, indirect or no relationship.

Independent variable has non-significant indirect effect on dependent variable through mediating variable in the absence of significant effect in path "a" and presents of significant effects in path "b" and "c". At the other side, independent variable has only a direct effect on dependent variable in the present of significant effect in path "a" and a none significant effect in path "b" or "c". There would be no any relationship between independent variable and dependent variable in the absence of significant relationship in path "a" and then absence of significant relationship in the paths "b" or "c".

The SEM technique is claimed to be preferable to regression techniques for testing mediation because SEM permit modelling of both measurement and structural relationships and yield overall fit indices (Browne & Cudeck, 1993; Garver & Mentzer, 1999). This research employed the bootstrapping approach (Bargozzi & Yi, 1988) to assess the mediating effects of Attitudes (AT).

The significance of the regression coefficients between Knowledge of Security Threat (KSTH), Knowledge of Organisation Information Security Strategy (KOISS), Knowledge of Security Technology (KSTG), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) as IVs, Attitudes (AT) as M and Behaviour (BH) as DV were examined to determine the occurrence of the mediation effect and its mediating degree. Thus, four hypotheses (i.e., H1.c, H2.c, H3.c, H4.c, H5.c and H6.c) were examined in this section. The results of examining these hypotheses are displayed in Table 6.10 with the standardized effects of different paths.

Table 6.10 Results of Examining Mediation Effects of Attitudes (AT)

DV = Behaviour (BH)	**Independent Variables (IVs)**					
	KSTH	**KOISS**	**KSTG**	**KLRNC**	**KSRS**	**KSRK**
Total Effect of IV on DV without M (path a)	$0.137^{**(sig:0.003)}$	$0.035^{(sig:0.489)}$	$0.067^{(sig:0.317)}$	$0.172^{*(sig:0.011)}$	$0.175^{**(sig:0.006)}$	$0.176^{**(sig:0.005)}$
Direct Effect of IV on DV with M (path a’)	$0.114^{*(sig:0.013)}$	$0.013^{(sig:0.737)}$	$0.039^{(sig:0.588)}$	$0.146^{*(sig:0.043)}$	$0.144^{*(sig:0.026)}$	$0.151^{*(sig:0.014)}$
Indirect Effect of IV on DV through M (path bc)	$0.024^{**(sig:0.002)}$	$0.022^{*(sig:0.010)}$	$0.029^{**(sig:0.011)}$	$0.026^{**(sig:0.009)}$	$0.031^{**(sig:0.005)}$	$0.025^{*(sig:0.012)}$
Effect of IV on M (path b)	$0.137^{**(sig:0.002)}$	$0.129^{*(sig:0.019)}$	$0.165^{*(sig:0.014)}$	$0.150^{*(sig:0.014)}$	$0.179^{**(sig:0.005)}$	$0.145^{*(sig:0.017)}$
Effect of M on DV (path c)	$0.174^{**(sig:0.004)}$	$0.174^{**(sig:0.004)}$	$0.174^{**(sig:0.004)}$	$0.174^{**(sig:0.004)}$	$0.174^{**(sig:0.004)}$	$0.174^{**(sig:0.004)}$
Mediation Path	KSTH→AT→BH	KOISS→AT→BH	KSTG→AT→BH	KLRNC→AT→BH	KSRS→AT→BH	KSRK→AT→BH

Mediation Effect	Yes	No	No	Yes	Yes	Yes
Degree of Mediation	Partial	---	---	Partial	Partial	Partial
Hypothesis Result	H1.c) Supported	H2.c) Rejected	H3.c) Rejected	H4.c) Supported	H5.c) Supported	H6.c) Supported

*p< 0.05 , **p< 0.01, ***p< 0.001

As shown in table 6.10, Attitudes (AT) mediates the effects of Knowledge of Security Threat (KSTH), Knowledge of Legislation, Regulation and National Culture (KLRNC), Knowledge of Security Responsibility (KSRS) and Knowledge of Security Risk (KSRK) on Behaviour (BH). Thus hypotheses H1.c, H4.c, H5.c and H6.c were supported. The following section discusses the results of the mediation analysis and indirect effects.

H1.c) Attitudes (AT) mediates the relationship between Knowledge of Security Threat (KSTH) and Behaviour (BH)

As shown in Table 6.10, the result showed that there was a significant relationship between Knowledge of Security Threat (KSTH) and Behaviour (BH) in the absence of Attitudes (AT), with the standardized total effect of 0.137 and the P-value of 0.003. Thus, the total effect of Knowledge of Security Threat (KSTH) as IV on Behaviour (BH) as DV without the inclusion of Attitudes (AT) as M was statistically significant at 0.01 level.

This relation was still significant even after inclusion Attitudes (AT) into the model, with the standardized direct effect of 0.114 and the P-value of 0.013. Thus, the direct effect of Knowledge of Security Threat (KSTH) as IV on Behaviour (BH) as DV with the inclusion of Attitudes (AT) as M was statistically significant at 0.05 level.

As depicted in Table 6.10, the effects of Knowledge of Security Threat (KSTH) as IV on Attitudes (AT) as M (path b) was statistically significant at 0.01 level, with the standardized effects of 0.137.

At the other side, the effects of Attitudes (AT) as M on Behaviour (BH) as DV (path c) was statistically significant at 0.01 level with the standardized effects of 0.174.

These results indicated that Attitudes (AT) mediates the relationship between Knowledge of Security Threat (KSTH) and Behaviour (BH). The degree of mediation was partial since the path a' (direct effect) was found as statistically significant. The phenomenon supported the hypothesis H1.c.

Furthermore, the result revealed that Knowledge of Security Threat (KSTH) had a significant indirect positive effect on Behaviour (BH) through Attitudes (AT) with the standardized indirect effect of 0.024, p-value = 0.002.

H2.c) Attitudes (AT) mediates the relationship between Knowledge of Organisation Information Security Strategy (KOISS) and Behaviour (BH)

As shown in Table 6.10, the result showed that there was no any significant relationship between Knowledge of Organisation Information Security Strategy (KOISS) and Behaviour (BH) in the absence of Attitudes (AT), with the standardized total effect of 0.035 and the P-value of 0.489. Thus, the total effect of Knowledge of Organisation Information Security Strategy (KOISS) as IV on Behaviour (BH) as DV without the inclusion of Attitudes (AT) as M was statistically insignificant. This phenomenon violated the presence of mediating effect of Attitudes (AT). Thus hypothesis H2.c was rejected.

Nevertheless, since the direct effect of Knowledge of Organisation Information Security Strategy (KOISS) as IV on Attitudes (AT) as M, as well as direct effect of Attitudes (AT) as M on Behaviour (BH) as DV were positively significant at 0.01, it can be stated that Knowledge of Organisation Information Security Strategy (KOISS) had significant positive indirect effect on Behaviour (BH) through Attitudes (AT); standard coefficient = 0.022, p-value = 0.010.

H3.c) Attitudes (AT) mediates the relationship between Knowledge of Security Technology (KSTG) and Behaviour (BH)

As shown in Table 6.10, the result showed that there was no significant relationship between Knowledge of Security Technology (KSTG) and Behaviour (BH) in the absence of Attitudes (AT), with the standardized total effect of 0.067 and the P-value of 0.317. Thus, the total effect of Knowledge of Security Technology (KSTG) as IV on Behaviour (BH) as DV without the inclusion of Attitudes (AT) as M was statistically insignificant.

This phenomenon violated the presence of mediating effect of Attitudes (AT). Thus hypothesis H3.c was rejected.

Nevertheless, since the direct effect of Knowledge of Security Technology (KSTG) as IV on Attitudes (AT) as M, as well as direct effect of Attitudes (AT) as M on Behaviour (BH) as DV were positively significant at 0.01. it can be stated that Knowledge of Security Technology (KSTG) had significant positive indirect effect on Behaviour (BH) through Attitudes (AT); standard coefficient = 0.029, p-value = 0.011.

H4.c) Attitudes (AT) mediates the relationship between Knowledge of Legislation, Regulation and National Culture (KLRNC) and Behaviour (BH)

As shown in Table 6.10, the result showed that there was a significant relationship between Knowledge of Legislation, Regulation and National Culture (KLRNC) and Behaviour (BH) in the absence of Attitudes (AT), with the standardized total effect of 0.172 and the P-value of 0.011. Thus, the total effect of Knowledge of Legislation, Regulation and National Culture (KLRNC) as IV on Behaviour (BH) as DV without the inclusion of Attitudes (AT) as M was statistically significant at 0.05 level.

This relation was still significant even after inclusion Attitudes (AT) into the model, with the standardized direct effect of 0.146 and the P-value of 0.043. Thus, the direct effect of Knowledge of Legislation, Regulation and National Culture (KLRNC) as IV on Behaviour (BH) as DV with the inclusion of Attitudes (AT) as M was statistically significant at 0.05 level.

As depicted in Table 6.10, the effects of Knowledge of Legislation, Regulation and National Culture (KLRNC) as IV on Attitudes (AT) as M (path b) was statistically significant at 0.05 level, with the standardized effects of 0.150.

Furthermore, the effects of Attitudes (AT) as M on Behaviour (BH) as DV (path c) was statistically significant at 0.01 level with the standardized effects of 0.174.

These results indicated that Attitudes (AT) mediates the relationship between Knowledge of Legislation, Regulation and National Culture (KLRNC) and Behaviour (BH). The degree of mediation was partial since the path a’ (direct effect) was found as statistically significant. The phenomenon supported the hypothesis H4.c.

Furthermore, the result revealed that Knowledge of Legislation, Regulation and National Culture (KLRNC) had a significant indirect positive effect on Behaviour (BH) through Attitudes (AT) with the standardized indirect effect of 0.026, p-value = 0.009.

H5.c) Attitudes (AT) mediates the relationship between Knowledge of Security Responsibility (KSRS) and Behaviour (BH)

As shown in Table 6.10, the result showed that there was a significant relationship between Knowledge of Security Responsibility (KSRS) and Behaviour (BH) in the absence of Attitudes (AT), with the standardized total effect of 0.175 and the P-value of 0.006. Thus, the total effect of Knowledge of Security Responsibility (KSRS) as IV on Behaviour (BH) as DV without the inclusion of Attitudes (AT) as M was statistically significant at 0.01 level.

This relation was still significant even after inclusion Attitudes (AT) into the model, with the standardized direct effect of 0.144 and the P-value of 0.026. Thus, the direct effect of Knowledge of Security Responsibility (KSRS) as IV on Behaviour (BH) as DV with the inclusion of Attitudes (AT) as M was statistically significant at 0.05 level.

As depicted in Table 6.10, the effects of Knowledge of Security Responsibility (KSRS) as IV on Attitudes (AT) as M (path b) was statistically significant at 0.01 level, with the standardized effects of 0.179.

Furthermore, the effects of Attitudes (AT) as M on Behaviour (BH) as DV (path c) was statistically significant at 0.01 level with the standardized effects of 0.174.

These results indicated that Attitudes (AT) mediates the relationship between Knowledge of Security Responsibility (KSRS) and Behaviour (BH). The degree of mediation was partial since the paths a’ (direct effect) was found as statistically significant. The phenomenon supported the hypothesis H5.c.

Furthermore, the result revealed that Knowledge of Security Responsibility (KSRS) had a significant indirect positive effect on Behaviour (BH) through Attitudes (AT) with the standardized indirect effect of 0.031, p-value = 0.005.

H6.c) Attitudes (AT) mediates the relationship between Knowledge of Security Risk (KSRK) and Behaviour (BH)

As shown in Table 6.10 the result showed that there was a significant relationship between Knowledge of Security Risk (KSRK) and Behaviour (BH) in the absence of Attitudes (AT), with the standardized total effect of 0.176 and the P-value of 0.005. Thus, the total effect of Knowledge of Security Responsibility (KSRS) as IV on Behaviour (BH) as DV without the inclusion of Attitudes (AT) as M was statistically significant at 0.01 level.

This relation was still significant even after inclusion Attitudes (AT) into the model, with the standardized direct effect of 0.151 and the P-value of 0.014. Thus, the direct effect of Knowledge of Security Risk (KSRK) as IV on Behaviour (BH) as DV with the inclusion of Attitudes (AT) as M was statistically significant at 0.05 level.

As depicted in Table 6.10, the effects of Knowledge of Security Risk (KSRK) as IV on Attitudes (AT) as M (path b) was statistically significant at 0.01 level, with the standardized effects of 0.145.

Furthermore, the effects of Attitudes (AT) as M on Behaviour (BH) as DV (path c) was statistically significant at 0.01 level with the standardized effects of 0.174.

These results indicated that Attitudes (AT) mediates the relationship between Knowledge of Security Risk (KSRK) and Behaviour (BH). The degree of mediation was partial since the paths a' (direct effect) was found as statistically significant. The phenomenon supported the hypothesis H6.c.

Further, the result revealed that Knowledge of Security Risk (KSRK) had a significant indirect positive effect on Behaviour (BH) through Attitudes (AT) with the standardized indirect effect of 0.025, p-value = 0.012.

6.7 Discussion on Hypothesis Testing

This study employed SEM for hypotheses testing, where the proposed research hypotheses were confirmed or rejected. The analysis was conducted to determine the answer to the third research question. As mentioned, for research hypotheses testing, the estimated coefficients (β), critical ratio (t-value) and significance level (p-value) were utilized in the study. Moreover, the estimated coefficients have to be distinct from zero and the t-value should exceed 1.96. Also, the level of significance should not exceed 0.05 or 0.01 according to Hair et al. (2006). Hence, for testing the research model of this study, the variables of the entire model were tested statistically and simultaneously.

Testing the hypothesis in the model aimed at identifying the level to which the model matched the study data. In this regard, adequate goodness-of-fit was determined to shed light on the plausibility of the tested variables proposed in the research model. With inadequate goodness-of-fit, the proposed relationships among the variables are deemed to be rejected (Byrne, 2013).

6.7.1 The Relationship between Security Knowledge Constructs and Attitude

The results regarding the relationships between security knowledge constructs and attitude were presented in section 6.6.1 and it is confirmed that H1a, H2a, H3a, H4a, H5a and H6a are accepted. The hypotheses respectively proposed the significant effect of knowledge of security threat (KSTH) on attitude (AT), knowledge of organisation information security strategy (KOISS) on attitude (AT), knowledge of security technology (KSTG) on attitude (AT), knowledge of legislation, regulation and national culture (KLRNC) on attitude (AT), knowledge of security responsibility (KSRS) on attitude (AT), and knowledge of security risk (KSRK) on attitude. Table 6.9 lists the support for the above hypotheses in the model. To conclude, statistically, there is a significant relationship between security knowledge constructs and attitude, indicating that when security knowledge constructs are instilled between organisation employees, their attitude is enhanced and strengthened.

Furthermore, the provision of security knowledge constructs to all employees will positively affect their attitudes concerning the knowledge of security threat, knowledge of organisation information security strategy, knowledge of their security responsibility, knowledge of security risks around them, knowledge of legislation, regulation and national culture, and knowledge of security technology. Consequently, such provision will change their attitudes to be more understanding and aware. This result matches those reported by studies in prior literature (e.g., der Linden, 2012; Khan, Alghathbar, Nabi & Khan, 2011; Kruger & Kearney, 2006; Veseli, 2011). Additionally, to protect confidential information assets, security education initiatives should be established to assist in changing the attitudes of managers and employees (Wilson & Hash, 2003). Hence, extensive degrees of security knowledge constructs inculcated to all employees are related to their improved attitude in protecting the information assets of the organisation.

This indicates that when management encourages and promotes awareness training program and knowledge concerning security knowledge constructs, this will support and modify employees' attitudes as a human firewall to safeguard the internal assets of the organisation. This is consistent with the interviewee of security experts that sated on the role of enhancing and changing the attitudes of employees. It is crucial for employees to know and understand why they can do and cannot do certain activities. As a result, providing security knowledge constructs to the employees will positively affect their attitudes to protect the organisation assets. It is pointless if human has knowledge but did not pose the appropriate attitude towards information security. This problem will lead to the ineffectiveness of information security and will contribute to the internal security incidents in organisation. Therefore, there is a need to emphasize on the importance of having the correct attitude towards information security in security education, and training program.

To clarify the positive relationship between security knowledge constructs and attitude between the employees in Palestinian healthcare organisations. The statistics provided by internet world stats in 2019 regarding Palestine, indicate there are increasing in internet use between the people in Palestine. This wide use for internet and spread use of smart phone between the employees to perform their tasks and their works in daily work routines lead the employees to know about the threats and new types of risks related to organisations information assets and personal data. Therefore, the employees become more aware and knowledge about threats, types threats, cybercrime, cyber security, the risks toward the organisation information assets, also the employees become more know about the international rules related to the protection of information laws, what they have to protect, how to protect and how they become part of protection process in their organisations. Therefore, the employee’s knowledge about security threat, knowledge of organisation information security strategy, knowledge of their security responsibility, knowledge of security risks around them, knowledge of legislation, regulation and national culture, and knowledge of security technology has positive affect on their attitudes toward protection of organisation assets. Consequently, such knowledge will change their attitudes to be more understanding and aware, which in turn help to influence the employee behaviour toward the protection of organisation information assets. On the basis of the present study’s findings, it is recommended that the management of organisations, particularly those in Palestinian healthcare sector should take the importance of security knowledge constructs into consideration to influence and enhance the employee attitudes toward the protection of organisation assets from inside. The benefits and opportunities can be determined through a pre- and post-application comparison.

6.7.2 The Relationship between Security Knowledge Constructs and Behaviour

The relationship results between security knowledge constructs and behaviour were presented in Section 6.6.1. It was evident that hypotheses H1b, H4b, H5b, and H6b were all supported. More specifically, the above hypotheses proposed significant effects of knowledge security threat (KSTH) on behaviour (BH), knowledge of legislation, regulation and national culture (KLRNC) on behaviour (BH), and knowledge of security risk (KSRK) on behaviour (BH). Table 6.9 confirms the support for H1b, H4b, H5b, and H6b in the model. This result supports other results in literature by Areej Al Hogail (2015); Rashid et al. (2013); Liebowitz & Wilcox (1997); Spijkervet (2005); Van Niekerk & Von Solms (2010); Topa & Karyda (2015); Blythe et al. (2015). However, hypotheses H2b and H3b were rejected as no statistical significant relationships were found between knowledge of organisation information security strategy (KOISS) and behaviour as well as knowledge of security technology (KSTG) and behaviour respectively.

Prior studies in literature revealed that knowledge alone is not the sole drivers of behaviour and these include Kaur & Mustafa (2013); Baranowski et al. (2003); Newbould & Furnell (2009). They explained that more than one variable influences behaviour. Experts’ feedback in the interviews that laid emphasis on security knowledge’s role in enhancing and changing employees' behaviour. Moreover, the employees have to be aware and understand why they have to follow the organisation information security strategy of what they can and cannot do. This supports the adoption of the KAB model in this study, where attitude is considered to have a mediating role in the knowledge-behaviour relationship. Based on the result of this study, the relationship between knowledge of organisation information security strategy and knowledge of security technology had a significant indirect positive effect on behaviour through attitude.

The rejection of hypotheses H2b and H3b may be attributed to the low knowledge of employees regarding the organisation's information security strategy, and security technology brought about by the complex security technology and the dynamic nature of technology in terms of hardware and software. For further explanations, Palestine is still under the Israeli occupation and this occupation put a lot of challenges on the technology use that help to protect the organisation and the information's. The Israeli occupation still close the borders crossing and have a full control on these borders. This will lead to have a negative consequences on the technologies use to protect the organisation assets in Palestine, which in turn lead Palestine to have a poor security infrastructure regarding the security technologies that help to protect the organisation assets. The main objective of occupation is to destroy all the existence of Palestinian peoples in Palestine. So, this will lead to negative impact on the technologies implemented to protect the organisations assets in Palestine. Based on the above, the Palestinian healthcare organisation as such part of organisations in Palestine lack to security technologies that help to protect the information, lack for security strategies, policies, actions or guidelines to protect the organisation information asset, and lack for appropriate security infrastructure to protect the organisation information assets. Therefore, there are no significant relationship between the employee's knowledge about security technology and employee's knowledge about organisation information security strategy to influence the employee behaviour as a case in Palestinian healthcare organisation. So these hypothesis were rejected.

In other hand, the hypotheses H1b, H4b, H5b, and H6b indicate there are significant effects on behaviour namely, knowledge security threat (KSTH) on behaviour (BH), knowledge of legislation, regulation and national culture (KLRNC) on behaviour (BH), knowledge of security risk (KSRK) on behaviour (BH), and knowledge of security responsibility (KSRS) on behaviour. To clarify, the increase wide use of internet in Palestine and its use to manage the works and tasks within organisations, also the wide use of smart devices among the employees within organisation for personal use or for organisational work use. This leads the employee to know about many security risks such as; threats, spyware, extortion, malicious code, phishing, hacking, etc., as a result from using the new technologies in organisations.

The increase of security incidents in organisations and cybercrime in Palestine lead the employee to become more aware and knowledge about the risks related to data protection and knowledge about the laws and regulations to data protection act. They also will be more knowledge about their responsibility toward protection of organisation asset and their personal data. These security knowledge has a significant impact on employee security behaviour towards the protection of organisation information assets. Every employee in organisation need to know about these security knowledge in order to protect their organisation assets. Therefore, understanding and applying security knowledge construct is vital. This implies that, employees must have an appropriate behaviour and attitude towards information security. Knowledge and behaviour should be in line so that the effectiveness of information security in organisation will be achieved.

This study recommends that owners/managers of Palestinian healthcare services should take into consideration the knowledge of organisation information security strategy and knowledge of security technology between the employees to change their behaviour. In other words, the employees should have sufficient knowledge about security knowledge construct that could change their attitudes, assumptions, views and knowledge as these would positively impact their behaviour to protect the organisation assets from inside (Alhogail, 2015; Da Veiga & Eloff, 2010; Kaur & Mustafa, 2013).

6.7.3 The Relationship between Attitudes and Behaviour

The result of the tested attitude-behaviour relationship was presented in Section 6.6.1, involving hypothesis H7 that proposed attitude has significant effect on behaviour. The model supported this hypothesis as evident from the values in Table 6.9. More specifically, statistically, a significant relationship exists between attitude and behaviour. That indicates the higher of employee's attitude towards security knowledge constructs, more positive behaviour would be. This result is aligned with those reported by prior studies such as Al-umaran (2015); Pattinson et al. (2016); Blythe et al.(2015).

Instilling appropriate attitude towards security knowledge constructs will lead to the effectiveness of information security and will contribute to minimize the internal security incidents in organisation. Therefore, there is a need to emphasize on the importance of instilling the desired attitude among the employees towards security knowledge construct in order to influence and enhance the employee behaviour.

According to the hypothesis result, it is recommended that owners/managers of Palestinian healthcare sector organisations that should pay attention to the attitudes among employees towards security knowledge construct in terms of threats, organisation information security strategy, security technology, legislation, regulation and national culture, security responsibility and security risk in order to influence their behaviour in a positive way.

6.7.4 The Relationship between Security Knowledge Constructs, Attitude and Behaviour

Section 6.6.2 presents the results regarding the relationship between security knowledge constructs, attitude and behaviour. It is evident that hypotheses H1c, H4c, H5c and H6c were supported. Specifically, the mentioned hypotheses proposed the mediating role of attitudes (AT) on the relationship between security knowledge's construct and behaviour such as attitudes mediating role on the relationship between knowledge of security threat (KSTH) and behaviour (BH), attitudes mediating role on the relationship between knowledge of legislation, regulation and national culture (KLRNC) and behaviour (BH), attitudes mediating role on the relationship between knowledge of security responsibility (KSRS) and behaviour (BH), and attitudes mediating role between the relationship of knowledge of security risk (KSRK) and behaviour (BH). Table 6.10 shows the support for these hypotheses in the study model. Added to this, the statistical results obtained confirmed a significant relationship between these security knowledge constructs and behaviour, with attitude as the mediating variable. Stated clearly, attitude (AT) partially mediated the relationship between security knowledge constructs (KSTH, KLRNC, KSRS and KSRK) and behaviour. Furthermore, the results revealed that the knowledge of security threat (KSTH), knowledge of legislation, regulation and national culture (KLRNC) and knowledge of security risk (KSRK) had a significant indirect positive effect on behaviour (BH) through attitudes (AT).

Furthermore, the result also indicated that the Attitudes (AT) cannot mediate the relationship between knowledge of organisation information security strategy (KOISS) and knowledge of security technology (KSTG)) to behaviour (BH). However, the knowledge of organisation information security strategy (KOISS) and knowledge of security technology (KSTG) had a significant indirect positive effect on behaviour through attitudes.

The above results imply that inculcating security knowledge constructs on employees will positively impact their attitudes towards them, which in turn, lead to a positive impact on their behaviour. This result matches with those reported in prior literature, for example, Veseli (2011); der Linden (2012); Bettinghaus (1986); Parsons et al.(2015); Kaur & Mustafa (2013); Khan et al. (2011).

The examination and testing of the proposed hypothesis shows the importance of attitude between the security knowledge constructs and behaviour. That means there are a significant indirect positive effect between the security knowledge's (KSTH, KOISS, KSTG, KSRK, KLRNC and KSRS) and behaviour. This increase that the organisations have to focus on attitude of employees to perform the desired behaviour. Therefore, this study recommends that owners/managers of Palestinian healthcare sector organisations to consider the importance of attitude in mediating the relationship between security knowledge constructs and behaviour among employees, and the indirect positive effect relationship through the attitudes. Promoting security knowledge awareness among employees should be practiced regularly as this will strengthen their attitudes and improve their behaviour when interacting with the information assets of the organisation. Thus, awareness of security knowledge should be promoted. This assumption matches the feedback provided by the interviewed experts who stressed on the importance of enhancing security knowledge to change the attitudes and then behaviour of employees. Furthermore, critical information assets of the organisation have to be protected by launching security education campaign as this would change the attitude and behaviour of managers and employees (Pattinson et al., 2016; Wilson & Hash, 2003).

6.8 Summary

In this research, data analysis was conducted in two major phases. The first phase involved a preliminary analysis of the data. This process is crucial to ensure that the data adequately meet the basic assumptions in using SEM. In general, the data set of all items was normally distributed and was free from failure, missing values and outliers. The second phase applied the two stages of SEM. The first stage included the establishment of measurement models for the latent constructs in the research. After confirming the uni-dimensionality, reliability and validity of the constructs in the first stage, the second stage was conducted to test the research hypotheses through developing the structural models.

Accordingly a structural model was developed to examine 13 hypothesized direct effects (i.e., H1.a, H2.a, H3.a, H4.a, H5.a, H6.a, H1.b, H2.b, H3.b, H4.b, H5.b, H6.b and H7) and 6 hypothesized mediation effects of Attitudes (i.e., H1.c, H2.c, H3.c, H4.c, H5.c and H6.c). These were done by conducting the path analysis using AMOS and testing the significant of the path coefficients for each hypothesized path.

The results indicated that knowledge of security threat (KSTH), knowledge of legislation, regulation and national culture (KLRNC), knowledge of security responsibility (KSRS) and knowledge of security risk (KSRK) had significant positive effects on Attitudes (AT) and Behaviour (BH). Further, knowledge of organisation information security strategy (KOISS) and knowledge of security technology (KSTG) had significant positive effects on Attitudes (AT) only. The effect of Attitudes (AT) on Behaviour (BH) was found as positively significant. Therefore, hypotheses H1.a, H2.a, H3.a, H4.a, H5.a, H6.a, H1.b, H4.b, H5.b, H6.b and H7 were supported.

From the results of mediation analysis it was found that Attitudes (AT) partially mediated the effects of knowledge of security threat (KSTH), knowledge of legislation, regulation and national culture (KLRNC), knowledge of security responsibility (KSRS) and knowledge of security risk (KSRK) on behaviour (BH). Thus, hypotheses H1.c, H4.c, H5.c and H6.c were supported. The results also indicated that knowledge of security threat

(KSTH), knowledge of organisation information security strategy (KOISS), knowledge of security technology (KSTG), knowledge of legislation, regulation and national culture (KLRNC), knowledge of security responsibility (KSRS) and knowledge of security risk (KSRK) had significant positive indirect effects on Behaviour (BH) through Attitudes (AT).

The last part of the chapter discussed the hypothesis relations between security knowledge construct's, attitude and behaviour. Finally, the study concludes the importance of conducting security knowledge awareness between the employees to influence their attitudes and their behaviour.

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 Summary of Research Findings

This study primarily aims to investigate the security knowledge constructs required to influence the employee's behaviour. This can then be used as a guide to organisations to instill the security knowledge required among the employees to influence their behaviour when interacting with information assets to minimize security risk. This section discusses the findings of this study in term of objective achievement. The discussions are based on the objectives of this study.

a. Research Objective 1: To identify the security knowledge construct required to influence employee behaviour.

The aim of this objective is to identify the security knowledge required to influence employee behaviour in organisation.

In chapter two, a literature review has been conducted to indicate the relationship between knowledge and behaviour in information security. We found there is a positive relationship between knowledge and behaviour. The level of knowledge significantly affects employee behaviour and should be considered as a critical factor in the effectiveness of information security culture. Thus, the chapter examined relevant studies to identify security knowledge constructs in an attempt to establish a link between organisation employee (i.e. insider) and security knowledge required to influence the behaviour. Furthermore, a discussion also provided to focus on insider threats to clarify the available sources of risk to information asset in organisation that couldn't be overlooked. The constructs are then confirmed by a group of security experts to support the findings obtained by the literature review.

The security knowledge constructs provided for organisation employees can work towards mitigating the threats in organisations and safeguarding information assets. Moreover, constructs of security knowledge assists in achieving the required behaviour of employees when they interact with the assets of the organisation. Organisational employees always have to be aware of these security knowledge and to achieve this, security knowledge has to be instilled in them. The organisation should provide security knowledge construct to employees to direct and manage their behaviour in their interaction with its assets.

The semi-structured interviews has been conducted by information security specialist to ensure all of these security knowledge constructs are relevant to help influence the employee behaviour in organisations, and to gain an in depth understanding of security knowledge constructs that are required to influence the employee behaviour in organisations. It also aims to obtain their opinions and feedbacks concerning knowledge needed to influence employee behaviour. The findings obtained from the interviews that all the interviewees confirmed that the security knowledge constructs are all relevant to help influence the employee behaviour in organisations.

More specifically, the findings of this objective is to identify the constructs of security knowledge required to influence employee behaviour namely knowledge of security threat, knowledge of organisational information security strategy, knowledge of security technology, knowledge of legislation, regulation and national culture, knowledge of security responsibility and knowledge of security risk.

This discussion answered the first research question that states, “What is the security knowledge construct required to influence employee behaviour?”

b. Research Objective 2: To propose a model for the relationship between security knowledge construct and employee behaviour.

The aim of this objective is to propose a model that depicts the relationship between knowledge and behaviour in order to determine the impact of security knowledge constructs to behaviour.

The second chapter provided an explanation of the relevant theories and models that address the relationship between knowledge and behaviour, and eventually to select a suitable model/theory to underpin the hypotheses of the study concerning security and knowledge.

In this study, security knowledge is extended to include six constructs to investigate their effect on employee behaviour. A model is proposed to examine the relation between knowledge-behaviour in this context, and from this examination, hypotheses are formulated to address the relationship between the constructs of security knowledge and behaviour. Identifying the above mentioned interconnections and to determine the effects of security knowledge on behaviour under question. Chapter five presents the research model and hypothesis developments.

Based on the review conducted on the relevant models to explain knowledge-behaviour relationship, the KAB (Knowledge, Attitude, Behaviour) model was found to be the most suitable model to represent the association among knowledge, attitudes and behaviour. The knowledge in KAB model has been extended into six constructs in order to identify the connections between the security knowledge construct and behaviour and to determine the impact each of security knowledge constructs on behaviour. A justification for selection this model is detailed in the fifth chapter. This discussion answered the second research questions that states, "How can the relationship between security knowledge construct and employee behaviour be presented?"

c. Research Objective 3: To determine the impact of each security knowledge constructs on employee behaviour.

The aim of this objective in this study is to determine the impact of each security knowledge constructs on behaviour. The model analysis presented in chapter six showed the hypothesis (H1.a, H2.a, H3.a, H4.a, H5.a, H6.a, H1.b, H4.b, H5.b, H6.b and H7) were supported, whereas H2.b and H3.b (knowledge of organisation information security strategy (KOISS) has significant effect on behaviour (BH) and knowledge of security technology (KSTG) has significant effect on behaviour (BH)) respectively, were rejected.

In the relation between knowledge of security constructs to attitude to behaviour. In other words, attitude (AT) mediates the effects of knowledge of security threat (KSTH), knowledge of legislation, regulation and national culture (KLRNC), knowledge of security responsibility (KSRS) and knowledge of security risk (KSRK) on behaviour (BH). Thus hypotheses H1.c, H4.c, H5.c and H6.c were supported. Whereas H2.c and H3.c (attitudes (AT) mediates the relationship between knowledge of organisation information security strategy (KOISS) and behaviour (BH), attitudes (AT) mediates the relationship between knowledge of security technology (KSTG) and behaviour (BH)) respectively, were rejected.

Nevertheless, since the direct effect of knowledge of organisation information security strategy (KOISS) as IV on attitudes (AT) as M, as well as direct effect of attitudes (AT) as M on behaviour (BH) as DV were positively significant at 0.01, it can be stated that knowledge of organisation information security strategy (KOISS) had significant positive indirect effect on behaviour (BH) through attitudes (AT). This same to H3.c, since the direct effect of knowledge of security technology (KSTG) as IV on attitudes (AT) as M, as well as direct effect of attitudes (AT) as M on behaviour (BH) as DV were positively significant at 0.01. It can be stated that knowledge of security technology (KSTG) had significant positive indirect effect on behaviour (BH) through attitudes (AT).

This answered the third research question of this thesis, namely: “What is the impact of each security knowledge construct to employee behaviour?”

7.2 Research Contributions

The work described in this thesis has made the following contributions to the field of information security management in general and to information security culture in particular. Specifically investigation on the relationship between security knowledge constructs and employee behaviour in organisations. In addition, this research also insights into the contributions in Arabic countries like Palestine. The theoretical and practical contributions of the study are listed as follows:

7.2.1 Theoretical Contributions

1. Enhancing theory of KAB model in information security.
2. Establishing principles and variables to study knowledge, attitude and behaviour in information security practices.
3. An extensive review of the literature on the cultivation of organisational information security culture is conducted to provide an overview of this research field, available frameworks, and methodologies used, and highlights the areas that may need further research in terms of information security culture for researchers.

4. This study attempted to bridge the gap in previous research through its investigation of the security knowledge constructs to improve the employee behaviour in information security culture that help and to influence the managers, professionals and organisations managements to establish information security culture in general and in Palestine specially as one of developing country. In spite of its global importance, there is a little studies focused on security knowledge constructs required to influence the employee behaviour that can help reduce the internal security incidents within an organisation and at the same time can increase the organisational effectiveness.

5. The findings of such research can be regarded as fundamental for future strategies in developing and establishing an information security culture with in organisations in general and in Palestinian's healthcare organisations specifically. That are characterized by poor information security culture. This means that a successful plan to protecting information assets from being disclosed, integrity violation, confidentially and denial of service. Therefore, the result will promote the stability and productivity of organisations and enhance the customer's trusts.
6. In addition, there are a few studies that investigated the security knowledge required to influence the employee's behaviour in developing countries such as Palestine. This study contributes and recommends that owners/managers of Palestinian healthcare services should take into consideration the findings of this study to improve their employee behaviour in healthcare organisations.
7. Based on literature review, this study is one of the genuine empirical studies that investigated the security knowledge constructs to influence the employee behaviour in healthcare services sector of the developing countries including Palestine.
8. This study intended to be a valuable source for further empirical and conceptual research for the implementation of information security culture with in organisations on the role security knowledge construct required to influence the employee's behaviour in other contexts. Besides its general contribution through identifying the security knowledge constructs and an investigation the impact of these security knowledge to behaviour, the results can be replicated for further investigation in a different sectors and field. It also provides further understanding of the security knowledge constructs, behaviour and attitude of the Palestinian healthcare owners/managers towards the protection of information.
9. The findings of the study guiding organisations, top management and professionals to provide a training awareness based on these security knowledge constructs, also its impact to the employee behaviour, that aim to guide the employee behaviour when interacting with information assets in order to protect the organisation information assets.
10. Further, this study encourage the organisations, top management and professionals to focus on the knowledge, attitude and behaviour in a providing training awareness

that to ensure to influence the employee behaviour. It is pointless if employee has knowledge but did not pose the appropriate attitude towards information security. This problem will lead to the ineffectiveness of information security and will contribute to the internal security incidents in organisation. Therefore, there is a need to emphasize on the importance of having the correct knowledge and attitude towards information security through security education, and training program.

11. This study concentrate the correlation between knowledge and behaviour in information security. Every employee need to know the importance of information security in order to protect their organisation assets. Therefore, understanding and applying security knowledge construct is vital. This implies that, employee must have appropriate behaviour and attitude towards information security. Knowledge and behaviour should be in line so that the effectiveness of information security in organisation will be achieved.
12. Users should be equipped properly to be protected. It is not enough to know about threats and why they are significant, for example, but they should be able to know what to do to protect themselves from these threats and how to use the related safeguards. This implies that the approach to awareness needs to be changed from just informing users about security issues to actually helping them to develop the ability to deal with them, i.e. create information security literacy among users by creating a baseline of information security culture.

7.2.2 Practical Contributions

1. This study takes into consideration the importance of cultivating security knowledge construct between the employees to guide their behaviour and to minimize the threat posed by them. It is one of the few earlier studies that focus between knowledge and behaviour in information security in healthcare services in Palestine.
2. The results of this study could be beneficial to policy makers in Palestine in that, implementing information security culture with in healthcare services would minimize the risk posed by the employee and keep the availability of information,

integrity of data and keep the confidentiality of the systems, which in turn, leads to improve healthcare services performance.

3. Decision makers in the healthcare service sector should make a comprehensive strategy for improving their employees' behaviour to protect the organisation information assets. The results of this study expected to help decision makers to structure their priorities in the instilling the security knowledge construct between the employees with in organisations. In order to improve the organisation performance, it is necessary to increase the employee behaviour level among the healthcare services sector.
4. In addition, healthcare services decision makers can benefit from the results of this study by providing a training awareness based on these security knowledge constructs, how to enhance the employee attitudes to specific behaviour in order to achieve the desired behaviour that aims to guide the employee behaviour when interacting with information assets in order to protect the organisation information assets.
5. It proposes the constructs of security knowledge required to influence employee behaviour with in organisation.
6. It determines the impacts of each security knowledge constructs to employee behaviour with in organisation.
7. It extends the knowledge in KAB model to include security knowledge constructs such as knowledge of security threat, knowledge of security technology, knowledge of organisation security policy, knowledge of security responsibility, knowledge of security risk, knowledge of legislation, regulation and national culture.
8. This thesis has presented a best practice guideline based on the security knowledge constructs and behaviour to guide practitioners when it comes to reviewing and cultivating the information security culture within different types of organisation. This guideline could be further investigated and developed to create a guide of reference or practical standards of an effective information security culture.
9. This research helps to provide structure and guidance to minimize the threats posed by employee behaviour to the security of organisation's information assets.

7.3 Limitations of the Research

This study has several limitations that need to be kept into consideration by future studies.

First, the result of this study are limited to healthcare organisations, particularly in Palestine. The result of this study may not be applicable to other sectors or countries. But the result does provide a guideline for such a study to be repeated in other sectors or countries.

Second, no data is available to verify the outcome of the study, since no empirical study has been conducted in this area. Such results would help the researcher to identify whether or not the security knowledge constructs can really provide a change in employee behaviour as expected. This was challenging due to the difficulty of getting organisation's approval to implement security knowledge construct within the limited timeframe of this research.

7.4 Recommendations for Future Research

The work presented in this thesis can be extended in the following ways:

1. To examine the impact of security knowledge construct required to enhance employee behaviour in light of information security culture in other sectors to generate domain-specific best practices.
2. To develop a computer application for the evaluation of the information security culture level in organisation on the basis of the security knowledge constructs. Such application may also be developed to determine the weaknesses and strengths of constructs in the quest to promote an effective information security culture.
3. To conduct assessment before and after the implementation of security knowledge constructs in the organisation. So that we can evaluate the strengths and weaknesses. This will provide an opportunity to assess recommendations arising from the evaluation of the information security culture in the organisation. Therefore, further research to study that is desirable.
4. Knowledge management could be integrated to develop a model that can assist organisations to efficiently cultivate the security knowledge required and predict how the information security culture could be improved. The knowledge management component could be used to capture, acquire and encode knowledge to help decision making. This model will definitely benefit from knowledge sharing

between organisations and will increase the efficiency of handling security incidents from insiders.

5. To replicate the research study in other sectors or countries with the aim to conduct a comparative analysis study. The findings can enrich the implementation of information security.

REFERENCES

Adler, N. J. (1983). A typology of management studies involving culture. *Journal of International Business Studies, 14*(2), 29–47.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, 107–136.

Al-Awadi, M., & Renaud, K. (2007). Success factors in information security implementation in organizations. In *IADIS International Conference e-Society*.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: a behaviour compliance conceptual framework. In *Proceedings of the Eighth Australasian Conference on Information Security-Volume 105* (pp. 47–55).

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. http://doi.org/10.1016/j.chb.2015.03.054

AlHogail, A., & Berri, J. (2012). Enhancing IT security in organizations through knowledge management. *2012 International Conference on Information Technology and E-Services, ICITeS 2012*, (January). http://doi.org/10.1109/ICITeS.2012.6216677

AlHogail, A., & Mirza, A. (2014). A proposal of an organizational information security culture framework. *Proceedings of International Conference on Information, Communication Technology and System (ICTS) 2014*, (JANUARY 2015), 243–250. http://doi.org/10.1109/ICTS.2014.7010591

Alhogail, A., & Mirza, A. (2014). Information Security Culture: A Definition and a Literature review. *Computer Applications and Information Systems (WCCCAIS)*, (January), 1–7. http://doi.org/10.1109/WCCAIS.2014.6916579

Alnatheer, M. A. (2014). A conceptual model to understand information security culture. *International Journal of Social Science and Humanity*, *4*(2), 104.

Alnatheer, M., & Nelson, K. (2009). Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. *Australian Information Security Management Conference*, (December), 6–17.

Al-umaran, S. (2015). Culture Dimensions of Information Systems Security in Saudi

Arabia National Health Services: A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy, (February), 167–171. Retrieved from https://www.dora.dmu.ac.uk/bitstream/handle/2086/11393/Thesis-1-June 2015-Final-v2.pdf?sequence=1&isAllowed=y

Alumaran, S., Bella, G., & Chen, F. (2015). Culture Dimensions of Information Systems Security in Saudi Arabia National Health Services. *International Journal O Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, *9*(2), 510–514. http://doi.org/http://dx.doi.org/10.5120/19639-1217

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise Management*, *6*(4), 279–314.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. http://doi.org/10.1016/j.chb.2014.05.046

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *British Journal of Social Psychology*, *40*(4), 471–499.

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201.

Authors, F. (2015). Information & Computer Security Article information : http://doi.org/http://dx.doi.org/10.1108/ICS-01-2015-0001

Awang, Z. (2012). *Structural equation modeling using AMOS graphic*. Penerbit Universiti Teknologi MARA.

Balnaves, M., & Caputi, P. (2001). *Introduction to quantitative research methods: An investigative approach*. Sage.

Baranowski, T., Cullen, K. W., Nicklas, T., Thompson, D., & Baranowski, J. (2003). Are current health behavioral change models helpful in guiding prevention of weight gain efforts? *Obesity Research*, *11*(S10), 23S–43S.

Bargozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation model. *Journal of Academy of Marketing Science*, *16*(1), 74–94.

Baron, R. M., & Kenny, D. A. (1986). The moderator--mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173.

Barzak, O., Molok, N. N. A., Talib, S., & Mahmud, M. (2017). Information security behavior among employees from the Islamic perspective. *Proceedings - 6th International Conference on Information and Communication Technology for the Muslim World, ICT4M 2016*, 211–215. http://doi.org/10.1109/ICT4M.2016.46

Baskerville, N. B., Hogg, W., & Lemelin, J. (2001). Process evaluation of a tailored multifaceted approach to changing family physician practice patterns improving preventive care. *The Journal of Family Practice*, *50*(3), W242–9.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61. http://doi.org/10.1016/j.chb.2015.01.039

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly*, 369–386.

Bentler, P. M. (1980). Multivariate analysis with latent variables: Causal modeling. *Annual Review of Psychology*, *31*(1), 419–456.

Bettinghaus, E. P. (1986). Health promotion and the knowledge-attitude-behavior continuum. *Preventive Medicine*, *15*(5), 475–491.

Bilal Khan. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862–10868. http://doi.org/10.5897/ajbm11.067

bin Othman Mustafa, M. S., Nomani Kabir, M., Ernawan, F., & Jing, W. (2019). An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks. *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS),* (June), 10–14. http://doi.org/10.1109/i2cacis.2019.8825070

Blunch, N. (2012). *Introduction to structural equation modeling using IBM SPSS statistics and AMOS*. Sage.

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance : The motivators and barriers of employees ' security behaviors. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 103–122.

Boujettif, M., & Wang, Y. (2010). Constructivist approach to information security awareness in the Middle East. In *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on* (pp. 192–199).

Božić, G. (2012). The role of a stress model in the development of information security culture. In *MIPRO, 2012 Proceedings of the 35th International Convention* (pp. 1555–1559).

Brady, J. W. (2011). Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on* (pp. 1–10).

Brenner, M. E. (2006). Interviewing in Educational Research. *Handbook of Complementary Methods in Education Research*, *2*, 357–370. http://doi.org/10.4135/9781473957602.n6

Browne, M. W., Cudeck, R., & others. (1993). Alternative ways of assessing model fit. *Sage Focus Editions*, *154*, 136.

Bryman, A., & Bell, E. (2015). *Business research methods*. Oxford University Press, USA.

Byrne, B. M. (2013). *Structural equation modeling with EQS: Basic concepts, applications, and programming*. Routledge.

Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. J. (2009). Common sense guide to prevention and detection of insider threats 3rd edition--version 3.1. *Published by CERT, Software Engineering Institute, Carnegie Mellon University, Http://www. Cert. Org*.

Cert, C. I. T. (2013). Unintentional insider threats: A foundational study. *Cahier de Recherche CMU/SEI-2013-TN-022, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA*, *18*.

Chang, S. E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107*(3), 438–458. http://doi.org/10.1108/02635570710734316

Chau, P. Y. K., & Hu, P. J.-H. (2001). Information technology acceptance by individual professionals: A model comparison approach. *Decision Sciences*, *32*(4), 699–719.

Chen, Y. A. N., Ramamurthy, K. R. A. M., & Wen, K. (2015). Impacts od Comprehensive Information Security Programs on Information Security Culture. *The Journal of Computer Information Systems*, *55*(3), 11. http://doi.org/10.1080/08874417.2015.11645767

Chia, P. a., Maynard, S. B., & Ruighaver, a. B. (2002). Understanding Organizational Security Culture. *Pacis*, 1–23. Retrieved from http://people.eng.unimelb.edu.au/seanbm/research/2003SecCultChap.pdf

Chin, W. W., & Newsted, P. R. (1999). Structural equation modeling analysis with small samples using partial least squares. *Statistical Strategies for Small Sample Research*, *1*(1), 307–341.

Chmura, J. (2017). Forming the Awareness of Employees in the Field of Information Security. *Journal of Positive Management*, *8*(1), 78. http://doi.org/10.12775/jpm.2017.006

Chua, Y. P. (2009). Statistik Penyelidikan Lanjutan Ujian Regresi, Analisis Faktor dan Ujian SEM. McGraw-Hill Malaysia.

Churchill Jr, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, 64–73.

Churchill, G. A. (2001). Title Basic Marketing Research. *The Dryden Press*, (Fort Worth).

Churchill, G. A., Brown, T. J., & Suter, T. A. (2004). *Basic marketing research*. Dryden Press Fort Worth, TX.

Coffman, D. L., & MacCallum, R. C. (2005). Using parcels to convert path analysis models into latent variable models. *Multivariate Behavioral Research*, *40*(2), 235–259.

Cohen, J. (1983). The cost of dichotomization. *Applied Psychological Measurement*, *7*(3), 249–253.

Colwill, C. (2009). Human factors in information security: The insider threat - Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196. http://doi.org/10.1016/j.istr.2010.04.004

Comrey, A. L., & Lee, H. B. (1992). A First Course in Factor Analysis (2nd edn.) Lawrence Earlbaum Associates. *Hillsdale, NJ*.

Conner, M. (2010). Cognitive determinants of health behavior. In *Handbook of behavioral medicine* (pp. 19–30). Springer.

Connolly, L., & Lang, M. (2013). Information Systems Security: The Role of Cultural Aspects in Organizational Settings. *Information Systems Security*.

Creswell, J. W. (2002). Educational research: Planning, conducting, and evaluating quantitative and qualitative research. Up~ per Saddle River, NJ: Merrill Prentice Hall. Dietrich, D. & Ralph, KS (1995). Crossing borders: Multicultural literature in the classroom. *The Journal of Educational Issues of Language Minority Students, 15*, 810–881.

Creswell, J. W. (2012). Collecting qualitative data. *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research. Fourth Ed. Boston: Pearson*, 204–235.

Creswell, J. W. (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches - John W. Creswell, J. David Creswell - Google Livros. Retrieved from https://books.google.pt/books?id=335ZDwAAQBAJ&printsec=frontcover&dq=research+design+qualitative+quantitative+and+mixed+methods+approaches&hl=pt-PT&sa=X&ved=0ahUKEwj12sClw6vbAhVHvhQKHQULCjkQuwUILjAA#v=onepage&q=research design qualitative quantitati

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101.

Da Veiga, A. (2008). Cultivating and Assessing Information Security Culture. *University Ot Pretoria.*

Da Veiga, A., & Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security*, *24*(2), 139–151.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. http://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162–176.

Da Veiga, A., Martins, N., & Eloff, J. H. P. (2007). Information security culture – validation of an assessment instrument. *South African Business Review*, *11*(1), 147–166.

Dattalo, P. (2008). *Determining sample size: Balancing power, precision, and practicality*. Oxford University Press.

der Linden, S. (2012). Understanding and achieving behavioural change: Towards a new model for communicating information about climate change. In *International*

Workshop on Psychological and Behavioural Approaches to Understanding and Governing Sustainable Tourism Mobility.

Detert, J. R., Schroeder, J. G., & Mauriel, J. J. (2000). A framework for linking culture and change initiatives in organizations. *Academy of Management Review*, *25*(4), 850–863.

DeVellis, R. F. (2016). *Scale development: Theory and applications* (Vol. 26). Sage publications.

Dhillon, G. (2007). *Principles of Information Systems Security: text and cases*. Wiley New York, NY.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125–128. http://doi.org/10.1145/341852.341877

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia. In *ECIS* (pp. 1560–1571).

Domanski, C. W. (2004). A biographical note on Max Friedrich (1856-1887), Wundt's first PhD student in experimental psychology. *Journal of the History of the Behavioral Sciences*, *40*(3), 311–317. http://doi.org/10.1002/jhbs.20022

Dörnyei, Z., & Taguchi, T. (2009). *Questionnaires in second language research: Construction, administration, and processing*. Routledge.

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. *Computer Fraud & Security*, *2005*(11), 10–16.

Eric Drever, S. C. for R. in E. (2003). *Using semi-structured interviews in small-scale research: a teacher's guide Número 129 de SCRE publication Volumen 15 de Practitioner minipaper*. ERIC.

Farrior, M. (2005). Break through strategies for engaging the public: emerging trends in communications and social science. Biodiversity Project.

FERNANDO, S. A. (2014). Internal Control of Secure Information and Communication Practices through Detection of User Behavioural Patterns.

Fishbein, M., & Ajzen, I. (1977). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. *Reading MA AddisonWeslet*, (3.8.2007), 480.

Flay, B. R., DiTecco, D., & Schlegel, R. P. (1980). Mass Media in Health Promotion: An Analysis Using an Extended Information-Processing Model. *Health Education & Behavior*, *7*(2), 127–147. http://doi.org/10.1177/109019818000700203

Flick, U. (2009). *An introduction to qualitative research*. Sage.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39–50.

Furnell, S. M., Clarke, N., von Solms, R., Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, *18*(5), 316–327.

Gable, G. G. (1994). Integrating case study and survey research methods: an example in information systems. *European Journal of Information Systems*, *3*(2), 112–126.

Gandhi, A. (2017). Quantitative assessment of information security awareness on informatics students in a university. *ACM International Conference Proceeding Series*, 346–350. http://doi.org/10.1145/3176653.3176728

Garver, M. S., & Mentzer, J. T. (1999). Logistics research methods: employing structural equation modeling to test for construct validity. *Journal of Business Logistics*, *20*(1), 33.

Glaser, B. G., & Strauss, A. L. (2009). *The discovery of grounded theory: Strategies for qualitative research*. Transaction publishers.

Graham, J. W., Hofer, S. M., Donaldson, S. I., MacKinnon, D. P., & Schafer, J. L. (1997). Analysis with missing data in prevention research. *The Science of Prevention: Methodological Advances from Alcohol and Substance Abuse Research*, *1*, 325–366.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis of unintentional insider threats deriving from social engineering exploits. In *Security and Privacy Workshops (SPW), 2014 IEEE* (pp. 236–250).

Groenewold, G., de Bruijn, B., & Bilsborrow, R. (2006). Migration of the Health Belief Model (HBM): effects of psychosocial and migrant network characteristics on emigration intentions in five countries in West Africa and the Mediterranean region.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., Tatham, R. L., & others. (1998). *Multivariate data analysis* (Vol. 5). Prentice hall Upper Saddle River, NJ.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., Tatham, R. L., & others. (2006). *Multivariate data analysis* (Vol. 5). Prentice hall Upper Saddle River, NJ.

Hair, J. F. J., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis Upper Saddle River: Pearson Prentice Hall.

Han, D. (2010). *The impact of salesperson's information overload on relationship selling behaviours and sales performance*. Auckland University of Technology.

Harrell, M. N. (2014). Factors impacting information security noncompliance when completing job tasks.

Hassan, N. H., & Ismail, Z. (2012). A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment. *Procedia - Social and Behavioral Sciences*, *65*, 1007–1012. http://doi.org/10.1016/j.sbspro.2012.11.234

Hayaati, N., Alwi, M., Fan, I., & Azni, A. H. (2015). Conceptual Study Towards Information Secuirty Model for E-learning Stakeholders, *10*(16), 7206–7211.

Hellriegel, D., Slocum, J. W., & Woodman, R. W. (1998). Organizational behavior. *ITP Nelson, Canada*.

Hepler, J. (2015). A good thing isn't always a good thing: Dispositional attitudes predict non-normative judgments. *Personality and Individual Differences*, *75*, 59–63.

Hicks, R. C., Dattero, R., & Galup, S. D. (2006). The five-tier knowledge management hierarchy. *Journal of Knowledge Management*, *10*(1), 19–31.

Ho, R. (2006). *Handbook of univariate and multivariate data analysis and interpretation with SPSS*. CRC Press.

Hogail, A. Al. (2015). Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study. *International Journal of Security and Its Applications*, *9*(7), 163–178. http://doi.org/10.14257/ijsia.2015.9.7.15

Howe, K., & Eisenhart, M. (1990). Standards for qualitative (and quantitative) research: A prolegomenon. *Educational Researcher*, *19*(4), 2–9.

Hoyle, R. H. (1995). *Structural equation modeling: Concepts, issues, and applications*. Sage.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660.

Huber, G. P. (1981). The nature of organizational decision making and the design of decision support systems. *MIS Quarterly*, 1–10.

Huczynski, A., & Buchanan, D. (2001). *Organizational Behaviour: An Introductory Text (Instructor's Manual)*. Financial Times/Prentice Hall.

Humaidi, N., & Balakrishnan, V. (2012). The influence of security awareness and security technology on users' behavior towards the implementation of health information system: A conceptual framework. In *2nd International Conference on Management and Artificial Intelligence IPEDR* (Vol. 35, pp. 1–6).

Ifinedo, P. (2014). The effects of national culture on the assessment of information security threats and controls in financial services industry. *International Journal of Electronic Business Management*, *12*(2), 75.

ISF. (2000). Information Security Forum. *Information Security Culture E a Preliminary Investigation*, *s1*(s1).

Ismail, M. B., & Yusof, Z. M. (2009). Demographic factors and knowledge sharing quality among Malaysian government officers. *Communications of the IBIMA*, *9*(1), 1–8.

Jakobsen, E., & Johansen, A. K. H. (2004). *"All I want is a system that works": evaluation of the health information system in Cape Town, South Africa--using an information audit to capture views from the grass root level*.

Jones, B. D. (1999). Bounded rationality. *Annual Review of Political Science*, *2*(1), 297–321.

Jöreskog, K. G., & Sörbom, D. (2010). *LISREL 8: Structural equation modeling with the SIMPLIS command language*. Scientific Software International.

Jouini, M., Rabai, L. B. A., & Aissa, A. Ben. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489–496. http://doi.org/10.1016/j.procs.2014.05.452

Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, *2013*, 286–290. http://doi.org/10.1109/ICRIIS.2013.6716723

Kelloway, E. K., Francis, L., Prosser, M., & Cameron, J. E. (2010). Counterproductive work behavior as protest. *Human Resource Management Review*, *20*(1), 18–25.

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3. In *Engineering* (Vol. 45, p. 1051). http://doi.org/10.1145/1134285.1134500

Kline, R. B. (2005). *Principles and practice of structural equation modeling*. Guilford publications.

Koh, K., Ruighaver, a., Maynard, S., & Ahmad, a. (2005). Security Governance : Its Impact on Security Culture. In *Proceedings of The third Australian Information Security Management Conference* (pp. 1–12). Retrieved from http://igneous.scis.ecu.edu.au/proceedings/2005/aism/koh.pdf

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, *38*(2), 143–154.

Krejcie, R. V, & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, *30*(3), 607–610.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296.

Kruger, H. A., & Kearney, W. D. (2008). Consensus ranking--An ICT security awareness case study. *Computers & Security*, *27*(7), 254–259.

Leonard, M., Graham, S., & Bonacum, D. (2004). The human factor: the critical importance of effective teamwork and communication in providing safe care. *Quality and Safety in Health Care*, *13*(suppl 1), i85–i90.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly*, 71–90.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394.

Liebowitz, J., & Wilcox, L. C. (1997). *Knowledge management and its integrative elements*. CRC Press.

Lilley, S., Lightfoot, G., & Amaral, P. (2004). *Representing organization: Knowledge, management, and the information age*. Oxford University Press.

Lim, J., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the relationship between organizational culture and information security culture. In *Proceedings of the 7th Australian Information Security Management Conference* (pp. 88–97). Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1011&context=ism

Liu, D., Wang, X., & Camp, L. J. (2009). Mitigating inadvertent insider threats with incentives. In *International Conference on Financial Cryptography and Data Security* (pp. 1–16).

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today’s reality, yesterday's understanding. *Mis Quarterly*, 173–186.

Lodico, M. G., Spaulding, D. T., & Voegtle, K. H. (2010). *Methods in educational research: From theory to practice* (Vol. 28). John Wiley & Sons.

Lomax, R. G., & Schumacker, R. E. (2012). *A beginner’s guide to structural equation modeling*. Routledge Academic New York, NY.

Longhurst, B., Smith, G., Bagnall, G., Crawford, G., Ogborn, M., Baldwin, E., … others. (2017). *Introducing cultural studies*. Routledge.

Lopes, I., & Oliveira, P. (2014). Understanding information security culture: a survey in small and medium sized enterprises. In *New Perspectives in Information Systems and Technologies, Volume 1* (pp. 277–286). Springer.

Lundy, M. O. (1993). Strategic human resource management.

Mäeses, S. (2015). Evaluation method for human aspects of information security. *Digi.Lib.Ttu.Ee*, 1–56. Retrieved from https://digi.lib.ttu.ee/i/?3582

Malcolmson, J. (2009). What is security culture? Does it differ in content from general organisational culture? In *43rd Annual 2009 International Carnahan Conference on Security Technology* (pp. 361–366).

Martins, A., & Elofe, J. (2002). Information security culture. In *Security in the information society* (pp. 203–214). Springer.

Mathieu, J. E., & Taylor, S. R. (2006). Clarifying conditions and decision points for mediational type inferences in organizational behavior. *Journal of Organizational Behavior*, *27*(8), 1031–1056.

McBurney, D. H., & White, T. L. (2009). *Research methods*. Cengage Learning.

McGuire, W. J. (1969). The nature of attitudes and attitude change. *Handbook of Social Psychology: The Individual in a Social Context (Vol. 3)*, *3*(2), 136–314.

McIntosh, B. (2011). An ethnographic investigation of the assimilation of new organizational members into an information security culture. Nova Southeastern University.

Merete Hagen, J., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management & Computer Security*, *17*(5), 388–407.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences*, *147*, 424–428. http://doi.org/10.1016/j.sbspro.2014.07.133

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, *43*(3), 449–473.

MOHAMAD RASHID, R., ZAKARIA, O., & NABIL ZULHEMAY, M. (2013). THE RELATIONSHIP OF INFORMATION SECURITY KNOWLEDGE (ISK) AND HUMAN FACTORS: CHALLENGES AND SOLUTION. *Journal of Theoretical & Applied Information Technology*, *57*(1).

Molok, A., Nuha, N., Chang, S., & Ahmad, A. (2013). Disclosure of organizational information on social media: Perspectives from security managers. *Disclosure*, *6*, 18–2013.

Myers, M. D., & others. (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, *21*(2), 241–242.

NCCIC. (2014). Combating the Insider Threat. *Natl. Cybersecurity Commun. Integr. Cent.*, p. 1.

Nelson, D. L., & Quick, J. C. (1996). *Organizational behavior: the essentials*. West Group.

Nelson, S. D., & Simek, J. W. (2002). Disgruntled Employees in Your Law Firm: The Enemy Within. *Neb. Law.*, 20.

Nelson, S. D., & Simek, J. W. (2006). Disgruntled Employees in Your Law Firm: The Enemy Within. *Wyo. Law.*, *29*, 22.

Newbould, M., & Furnell, S. (2009). Playing Safe: A prototype game for raising awareness of social engineering. In *Australian Information Security Management Conference* (p. 4).

Ng, B. Y. (2007). 31 . Studying Users ' Computer Security Behavior Using the Health Belief Model. *Information Systems*, (Rhodes), 423–437.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825.

Ngo, L., Zhou, W., & Warren, M. (2005). Understanding Transition towards Information Security Culture Change. In *Proceeding of the 3rd Australian Computer, Network & Information Forensics Conference, Edith Cowan University, School of Computer and Information Science* (pp. 67–73). Retrieved from http://84.205.229.18/securityc/d/english/Culture/Understanding Transition towards Information Security Culture Change.pdf

Niekerk, J. Van, & Solms, R. Von. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. *Issa*, 1–13.

Niekerk, J. Van, & Solms, R. Von. (2006). Understanding Information Security Culture. *Proceedings of the ISSA 2006 from Insight to Foresight Conference*.

Nonaka, I., & Takeuchi, H. (1995). *Knowledge-creating Company: How Japanese Companies Create the Dynamics of Innovation*. Oxford university press.

Nunnally, J., & Bernstein, L. (1994). Psychometric theory. New York: McGraw-Hill Higher, INC; *Intentar Embellecer Nuestras Ciudades Y Tambi{é}n Las*.

Nunnally, J. C., & Bernstein, I. H. (1994). Psychological theory. *New York, NY: MacGraw-Hill*.

Oates, B. J. (2006). *Researching information systems and computing*. Sage.

OECD. (2005). OECD; 2005. In *The promotion of a culture of security for information systems and networks in OECD countries (OECD)*. Retrieved from www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

Okere, I., Van Niekerk, J., & Carroll, M. (2012). Assessing information security culture: A critical analysis of current approaches. In *2012 Information Security for South Africa* (pp. 1–8).

Oppenheim, A. N. (2000). *Questionnaire design, interviewing and attitude measurement*. Bloomsbury Publishing.

Orozco, J., Tarhini, A., & Tarhini, T. (2015). A framework of IS/business alignment management practices to improve the design of IT Governance architectures. *International Journal of Business and Management*, *10*(4), 1.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117–129. http://doi.org/10.1177/1555343415575152

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. http://doi.org/10.1016/j.cose.2013.12.003

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: a comparison of two studies. *Information and Computer Security*, *24*(2), 228–240. http://doi.org/10.1108/ICS-01-2016-0009

Paulsen, C., & Coulson, T. (2011). Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security. *Communications of the IIMA*, *11*(3).

Payne, D. A. & McMorris, R. F. (1967). No TEducational and Psychological Measurement: Contributions to Theory and Practiceitle. *Waltham, Mass: Blaisdell Publication.*, (2nd Ed.).

PHIC. (2016). Palestinian Health Information Center, (2016).

Pinsonneault, A., & Kraemer, K. (1993). Survey research methodology in management information systems: an assessment. *Journal of Management Information Systems*, *10*(2), 75–105.

Pipkin, D. L. (2000). *Information security: protecting the global enterprise*. Prentice Hall PTR.

Ponemon Insitute. (2016). Cost of Data Breach Study: Global Analysis, (May), 1–30. Retrieved from https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

Pwc. (2013). State of Cybercrime Survey 2013, p.20.

Quaddus, M., & Hofmeyer, G. (2007). An investigation into the factors influencing the adoption of B2B trading exchanges in small businesses. Springer.

Raitoharju, R., Heiro, E., Kini, R., & D'Cruz, M. (2009). Challenges of Multicultural Data Collection and Analysis: Experiences From the Health Information System Research. *Electronic Journal of Business Research Methods*, *7*(1).

Rashid, R. M., Zakaria, O., & Zulhemay, N. (2014). Australian Journal of Basic and Applied Sciences Determining critical success factors (CSF) of information security knowledge (ISK) towards organisations ' information security effectiveness, *8*(23), 336–344.

Rashid, R. M., Zakaria, O., & Zulhemay, N. M. (2013). the Relationship of Information Security Knowledge (Isk) and Human Factors : Challenges and Solution. *Journal of Theoretical and Applied Information Technology*, *57*(1).

Renaud, K., & Goucher, W. (2014). The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 361–372).

Richardson, R. (2007). The CSI Computer Crime and Security Survey.[Online] http://i. cmpnet. com/v2. gocsi. com/pdf. *CSISurvey2007. Pdf*.

Ringle, C. M., Wende, S., & Becker, J.-M. (2015). SmartPLS 3. Boenningstedt: SmartPLS GmbH.

Robbins, S. P. (2001). *Organisational behaviour: global and Southern African perspectives*. Pearson South Africa.

Rogers, L. (2002). Home Computer Security. *CERT Coordination Centre*.

Rosenstock, I. M. (1960). What research in motivation suggests for public health. *American Journal of Public Health and the Nations Health*, *50*(3_Pt_1), 295–302.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56–62.

Rutherford, G. S. W., Hair, J. F., Anderson, R. E., & Tatham, R. L. (1988). Multivariate Data Analysis with Readings. *The Statistician*, *37*(4/5), 484. http://doi.org/10.2307/2348783

Sabbagh, B. Al, Ameen, M., Wätterstam, T., & Kowalski, S. (2012). A Prototype For HI ^{2} Ping Information Security Culture and Awareness Training. In *e-Learning and e-Technologies in Education (ICEEE), 2012 International Conference on* (pp. 32–36).

Sabeeh, A., & Lashkari, A. H. (2011). Users' perceptions on mobile devices security awareness in Malaysia. In *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for* (pp. 428–435).

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*. http://doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. http://doi.org/10.1016/j.chb.2015.12.037

Samy, G. N., Ahmad, R., & Ismail, Z. (2009). Threats to health information security. In *Information Assurance and Security, 2009. IAS'09. Fifth International Conference on* (Vol. 2, pp. 540–543).

Saunders, M. N. K. (2011). *Research methods for business students, 5/e*. Pearson Education India.

Schein Edgar, H. (1992). Organizational culture and leadership. *Jossey-Bass, San Francisco Google Scholar*.

Schlienger, T., & Teufel, S. (2003). Information security culture-from analysis to change. *South African Computer Journal*, (31), p–46.

Schumacker, R. E., & Lomax, R. G. (2004). *A beginner's guide to structural equation modeling*. Psychology Press.

Schwab, D. P. (2013). *Research methods for organizational studies*. Psychology Press.

Sekaran, Uma and Bougie, R. (2016). *Research Methods for Business: A Skill Building Approach*. John Wiley & Sons.

Sekaran, U. (2016). Research methods for business: A skill building approach.

Shahri, A. B., Ismail, Z., & Rahim, N. Z. A. (2013). Security culture and security awareness as the basic factors for security effectiveness in health information systems. *Jurnal Teknologi (Sciences and Engineering)*, *64*(2), 7–12. http://doi.org/10.11113/jt.v64.2212

Sherif, E., Furnell, S., & Clarke, N. (2015). An identification of variables influencing the establishment of information security culture. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 436–448).

Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, *69*(1), 99–118.

Singh, P., Chan, Y. F., & Sidhu, G. K. (2006). *A comprehensive guide to writing a research proposal*. Venton.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. In *IFIP International Information Security Conference* (pp. 133–144).

Slater, S. F. (1995). Issues in conducting marketing strategy research. *Journal of Strategic Marketing*, *3*(4), 257–270.

Smircich, L. (1983). Concepts of culture and organizational analysis. *Administrative Science Quarterly*, 339–358.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security, 56*, 1–13. http://doi.org/10.1016/j.cose.2015.10.006

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124–133. http://doi.org/10.1016/j.cose.2004.07.001

Straub, D. W., Loch, K. D., & Hill, C. E. (2003). Transfer of information technology to the Arab world: a test of cultural influence modeling. *Advanced Topics in Global Information Management*, *2*, 141–172.

Syed Ikhsan, S. O. S. (2005). *Knowledge management in a public organisation: a study of the performance of knowledge transfer in the Ministry of Entrepreneur Development of Malaysia*. {\copyright} Syed Omar Sharifuddin Syed Ikhsan.

Symantec. (2017). ISTR. Internet Security Threat Report. Volume 22, (April). http://doi.org/10.1016/S1353-4858(05)00194-7

Symantec. (2018). Internet Security Threat Report, *23*(March). Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Tabachnick, B. G. (2001). Clearing Up Your Act: Screening Data Prior to Analysis, Tabachnick, BG & Fidell, LS (eds), Using Multivariate Statistics. Harper Collins, New York.

Thomson, K.-L., Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11. http://doi.org/http://dx.doi.org/10.1016/S1361-3723(06)70430-4

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security*, *6*(4), 167–173.

Topa, I., & Karyda, M. (2015). Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance. In *International Conference on Trust and Privacy in Digital Business* (pp. 169–179).

Trochim, W. M. K. (2006). Types of reliability. Research methods knowledge base. *Web Center for Social Research Methods. Http://www. Socialresearchmethods. Net/kb/reltypes. Php*.

van der Spek, R., & Spijkervet, A. (1997). Knowledge management: Dealing Intelligently with Knowledge. *The Annals of Occupational Hygiene*, *49*(6), 543. http://doi.org/10.1093/annhyg/mei026

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers and Security*, *29*(4), 476–486. http://doi.org/10.1016/j.cose.2009.10.005

Verizon. (2014). 2014 Data Breach Investigations Report. *Verizon Business Journal*, *2014*(1), 1–60. Retrieved from file:///C:/Users/Edward S. Forde/Downloads/rp_Verizon-DBIR-2014_en_xg.pdf

Veseli, I. (2011). Measuring the Effectiveness of Information Security Awareness Program. *Information Security*.

Von Solms, B. (2006). Information security--the fourth wave. *Computers & Security*, *25*(3), 165–168.

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security*, *23*(4), 275–279.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191–198.

Walker, L. R., & Thomas, K. W. (1982). Beyond expectancy theory: An integrative motivational model from health care. *Academy of Management Review*, *7*(2), 187–194.

Warkentin, M., Straub, D., & Malimage, K. (2012). Measuring secure behavior: A research commentary. *Annual Symposium on Information Assurance & Secure Knowledge Management*, 1–8.

Warkentin, M., Straub, D., & Malimage, K. (2012). Measuring secure behavior: A research commentary. In *Proceedings of the annual symposium on information assurance* (pp. 1–8).

Watson, J. (2001). How to Determine a Sample Size. *Program Evaluation Tipsheet #60*, 5. Retrieved from http://www.extension.psu.edu/evaluation/pdf/TS60.pdf

Whiteman, M. E., & Matort, H. J. (2014). *Principles of Information Security*. Cengage Learning.

Whitman, M., & Mattord, H. (2013). *Management of information security*. Nelson Education.

Williams, P. (2009). What does security culture look like for small organizations? *Australian Information Security Management Conference*, (December), 48–54. Retrieved from http://ro.ecu.edu.au/ism/7/

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special Publication*, *800*, 50.

Wimmer, R. D., & Dominick, J. R. (2006). *Mass media: metody bada{ń}*. Wydawnictwo Uniwersytetu Jagiello{ń}skiego.

Woon, I., Tan, G.-W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 Proceedings*, 31.

Yin, K. R. (2003). Case Study Research: Design and Methods:(Applied Social Research Methods, Sage).

Zakaria, O. (2004). Understanding Challenges of Information Security Culture: A Methodological Issue. In *In the 2nd Australian Information Security Management Conference, Securing the Future.* (pp. 83–93.). Perth, Australia.

Zakaria, O. (2006). Internalisation of information security culture amongst employees through basic security knowledge. *IFIP International Federation for Information Processing*, *201*, 437–441. http://doi.org/10.1007/0-387-33406-8_38

Zakaria, O. (2007). Investigating information security culture in a public sector organisation : challenges Malaysian a case, (June), 1 – 200.

APPENDIX A.
ARABIC QUESTIONNAIRE

بسم الله الرحمن الرحيم،،،

السلام عليكم ورحمة الله وبركاته..
تحية طيبة وبعد،،

إذ يثمن الباحث موافقتكم الكريمة على المشاركة في هذه الإستبانة والتي تهدف الى قياس مستوى ثقافة أمن المعلومات لدى الموظفين في المؤسسة من اجل تطوير والحفاظ على أمن المعلومات فيها. وقياس أثر المعرفة الامنية في أمن المعلومات على السلوك الأمني لدى الموظفين. وهي جزء من بحث لنيل درجة الدكتوراه في ادارة أمن المعلومات.

الاستبانة موجهه لجميع موظفي المؤسسة في مختلف التخصصات. ستكون جميع المعلومات سرية ولن يدلى باسم المؤسسة اثناء عرض النتائج كما لن يطلع عليها أحد سوى الفريق البحثي .معلوماتكم الشخصية ستستخدم لغرض التصنيف فقط وستبقى هويتكم مجهولة.

مشاركتكم ستساهم في الحصول على نتائج دقيقه تخدم البحث العلمي لإرتقاء بمستوى أمن المعلومات في المؤسسات المختلفة في فلسطين.

شكرا لتعاونكم مرة أخرى، وإذا كان لديكم أي استفسارات فلا تترددوا بالتواصل معنا،،،

أمجد محفوظ
قسم ادارة أمن المعلومات
College of Computer Science & Information Technology
Tenaga National University
amahfouth99@gmail.com

القسم الاول : البيانات الشخصية :

يحتوى هذا القسم على سبعة بنود تعكس معلومات عامة عن المشاركين. من فضلك ضع الرمز (√) في الخانه المناسبة

1. **(العمر) :**

□ Under 25 □ 25 - 35 □ 36 - 45 □ Above 45

2. **(سنوات الخبرة) :ما عدد سنوات العمل في المؤسسة؟**

□ Less than a year □ 2 - 4 Years □ 5 - 10 Years
□ More than

3. **(طبيعة العمل) :ما طبيعة عملك؟**

□ Nurse □ Hospital Management □ Doctor
□ Administartive Staff

4. **(المؤهل العلمي) :**

□ Undergraduate(بكالوريس) □ Postgraduate(درلسات عليا)

5. **Gender (الجنس) :**

□ Male(ذكر) □ Female(أنثى)

6. **هل تعمل في قسم الحاسوب أو تكنولوجيا المعلومات في المؤسسة ؟**

□ Yes(نعم) □ No(لا)

7. **هل كانت دراستك في مجال الحاسوب او لها علاقة بتكنولوجيا المعلومات؟**

□ Yes(نعم) □ No(لا)

8. هل طبيعة عملك تتطلب استخدام الحاسوب؟

□ Yes(نعم) □ No(لا)

9. هل حصلت على دورات عن التوعية الأمنية حول أمن المعلومات؟

□ Yes(نعم) □ No(لا)

القسم الثاني : انواع المعرقة الامنية المطلوبة في المؤسسة من اجل تحسين سلوك الموظفين.

يهدف هذا القسم الى إختبار مجموعة من المعرفة الامنية المطلوية وذلك من اجل تحسين السلوك الامني للموظفين. ما هي انواع المعرفة الامنية المطلوبة التي تؤثر على السلوك الامني للموظفين في كل قسم .من فضلك ضع اشارة (√) في الخانه المناسبه.

No.	الفقرات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
المعرفة حول التهديدات الامنيKnowledge of Security Threat						
.1	لدي معرفة حول انواع التهديدات الالكترونية الضارة المتعلقة بأصول المعلومات.					
.2	مدرك بالنتائج السلبية للهجوم والتهديدات الالكترونية على أصول المعلومات.					
.3	مدرك بان التهديدات والهجمات الالكترونية يمكن ان تحدث في اي وقت					
.4	مدرك بالتهديدات الالكترونية والثغرات الامنية تجاه اصول المعلومات في بيئة العمل.					
.5	مدرك بالتهديدات المتعلقة بأمن المعلومات.					
المعرفة حول استراتيجية امن المعلومات للمؤسسة (سياسة امن ألمعلومات المقاييس والعمليات الامنية المطلوبة)						
.6	لدي معرفة بإستراتيجية امن المعلومات في المؤسسة.					
.7	سياسة امن المعلومات في المؤسسة تساهم في حماية اصول المعلومات					
.8	مدرك بعناصر استراتيجة امن المعلومات في المؤسسة مثل السياسات الامنية الموجودة					
.9	مدرك بان استراتيجية امن المعلومات للمؤسسة تساعدني في معرفة ما هو المتوقع مني لحماية اصول المعلومات فيها.					
.10	أعتقد بان المؤسسة طورت استراتيجية امن المعلومات للمساعدة في منع واكتشاف التهديدات الامنية والرد عليها ومقاومتها.					
.11	مدرك بأهمية متطلبات امن المعلومات لحماية اصول المعلومات في المؤسسة					
.12	مدرك لسياسات امن المعلومات المرتبطة في عملي مثل السياسية المتعلقة في كلمة المرور.					
.13	امن المعلومات ضروري لحماية المعلومات في المؤسسة.					
.14	امن المعلومات ضروري لزيادة ثقة الجهات الخارجية للمؤسسة.					
.15	لدي معرفة بالممارسات المتعلقة بأمن المعلومات مثل ضرورة تشفير البيانات وترميزها.					
.16	مدرك للممارسات المتعلقة بأمن المعلومات مثل عدم ترك اوراق مهمة في المكتب.					
.17	لدي معرفة حول ضوابط امن المعلومات مثل الحفاظ على كلمات مرور معقدة.					
.18	لدي معرفة بان تحقيق متطلبات امن المعلومات تساعدني في حماية اصول المعلومات في المؤسسة.					
Knowledge of Security Technology المعرفة حول التكنولوجيا الامنية						
.19	لدي معرفة بأن الأدوات التقنية والضوابط المستخدمة في امن المعلومات تساعدني في الحفاظ على معلومات المؤسسة.					
.20	معرفتي في التقنيات الامنية تمكنني من مساعدة الموظفين في المؤسسة للإجابة عن استفساراتهم ومشاكلهم التقنية					

No.	الفقرات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
21.	مدرك بان الاستخدام المناسب للضوابط التقنية (الفنية) يساهم في تحقيق امن المعلومات للمؤسسة.					
22.	المعرفة في السياسات والإرشادات حول الاستخدام الفعال لتقنيات وبرمجيات امن المعلومات تساهم في الحفاظ على امن المعلومات ومنع التهديدات والخروقات الامنية.					
23.	مدرك بأهمية استخدام التدابير الامنية مثل برامج مكافحة الفيروسات لتحقيق امن المعلومات في المؤسسة					
Knowledge of legislation, regulations, national culture such as act Data Protection Acts, HIPPA, International Standards etc. المعرفة في اللوائح والتشريعات القانونية لحماية المعلومات وأمنها						
24.	لدي معرفة باللوائح الحكومية المتعلقة في امن المعلومات.					
25.	مدرك للتشريعات الحكومية المتعلقة بأمن المعلومات مثل حقوق النسخ والنشر.					
26.	مدرك للوائح والتشريعات المتعلقة في قانون حماية البيانات.					
27.	مدرك للوائح والتشريعات المتعلقة في قانون الخصوصية وغيرها					
28.	لدي توجيهات واضحة حول حماية المعلومات الحساسة والسرية وتطبيق اللوائح المتعلقة بها.					
29.	مدرك لأهمية الحفاظ على قيم الملكية الفكرية وقانون حقوق النسخ.					
30.	أعلم بان عملية أمن المعلومات لا ينبغي أن تتعارض مع أخلاقيات المجتمع وقيمه الاساسية.					
31.	لدي معرفة بان مفهوم الثقافة الوطنية يجب ان يؤخذ بعين الاعتبار عند تصميم سياسة خطة أمن المعلومات.					
32.	لدي معرفة بان اجراءات امن المعلومات في المؤسسة يجب ان تتوافق مع المعايير العالمية المتبعة.					
المعرفة المتعلقة في المسؤولية الامنية للأفراد **Knowledge of Security Responsibility**						
33.	مدرك بأن امن المعلومات هي من ضمن مسؤوليتي في المؤسسة.					
34.	مدرك أنني مسؤول عن أي إجراء يتعارض مع متطلبات أمن المعلومات في المؤسسة.					
35.	اعرف ما هو المقصود في امن المعلومات.					
36.	لدي معرفة عن كيفية الابلاغ عن اي حادث متعلق في امن المعلومات.					
37.	اعرف ما هو دوري فيما يتعلق بالسياسات الامنية في المؤسسة.					
38.	مدرك ما يجب القيام به عندما كشف عن اي انتهاك أمان في المؤسسة.					
39.	انا على معرفة حول اصول المعلومات التي يجب حمايتها وكيف اعمل على حمايتها.					
40.	اعرف مدى اهمية حماية اصول المعلومات في المؤسسة لتحقيق نجاح الاعمال فيها.					
41.	انا مدرك جدا عدم الافصاح عن كلمة المرور الخاصة بي لأي شخص كان.					
المعرفة حول المخاطر الامنية **Knowledge of Security Risk**						
42.	انا مدرك بان كلمات المرور الضعيفة تعرضني للخطر.					
43.	انا مدرك للمخاطر الناتجة عن فتح وصلات المواقع (الارتباطات Links).					
44.	انا على مدرك بالمخاطر الامنية الضارة حول اصول المعلومات في بيئة عملي					
No.	الفقرات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
45.	انا على معرفة بالمخاطر الناتجة عن فتح رسائل من اشخاص مجهولين خاصة عند فتح المرفقات.					

46.	انا مدرك بالمخاطر الامنية الناتجة عن مشاركة وتبادل كلمات المرور بين الاخرين في العمل.					
47.	انا مدرك علم بالمخاطر الامنية الناتجة عن اعطاء معلومات حساسة لاحدى مواقع الانترنت العامة التي يحظر زيارتها.					
48.	يجب ان اكون على حذر عند الحديث عن معلومات سرية في الاماكن العامة.					

القسم الثالث : السلوك الامنى للموظفين داخل المؤوسسة.

يهدف هذا القسم الى إختبار مجموعة من السلوك الامنى لدى الموظفين وذلك من اجل حماية المؤسسة من الداخل والقيام بالمهام الامنية المطلوبة. ما هو العامل الامني المطلوب لحماية المؤسسة .من فضلك ضع اشارة (√) في الخانه المناسبه.

السلوك الامني للموظفين في المؤسسة Security Behaviour						
49.	احدث برامج مضادات الفايروسات في المؤسسة بشكل منظم.					
50.	اغلق حاسوبي عند مغادرة مكتبي.					
51.	اتاكد من عدم جود اوراق مهمة على المكتب عند مغادرة مكتبي.					
52.	عندما اشعر بوجد اختراق في المعلومات ابلغ عنه فورا.					
53.	يجب ان اتصرف بطريقة ملائمة تمنع اي تهديد على امن المعلومات في المؤسسة.					
54.	اشارك الموظفين بالمعلومات المتعلقة في التهديدات والثغرات الامنية.					
55.	انا التزم بمتطلبات امن المعلومات داخل المؤسسة.					
56.	اتصرف بطريقة فاعلة لاكتشاف والرد على اي اختراق للمعلومات في المؤسسة.					
57.	اتصرف بعناية عند فتح مرفقات الرسائل خاصة عند استلام رسائل من مجهولة المصدر.					
58.	استطيع ان اسال بسهولة واستفسر عن اي شيء يتعلق بأمن المعلومات.					
59.	اتبع استراتيجيات أمن المعلومات في المؤسسة في الاعمال اليومية لحماية اصول المعلومات.					
60.	لدي كلمة مرور قوية.					
61.	لا افتح مرفقات اي رسالة اذا كانت الرسالة تحتوي على اشياء مشكوك بها او مشبوهة.					
62.	قبل فتح اي رسالة اركز اولا في محتوى العنوان و مصدر الرسالة.					
63.	لا افصح عن اي معلومات شخصية متعلقة بي لمواقع غير معروفة وغير امنة.					

القسم الرابع : المواقف والاتجاهات

يهدف هذا القسم الى النعرف على مواقف واتجاهات الموظفين حول معرفتهم باتواع المعرفة الامنية المطلوبة وذلك من اجل تحسين سلوكهم الامني في المؤسسة .من فضلك ضع اشارة (√) في الخانه المناسبه.

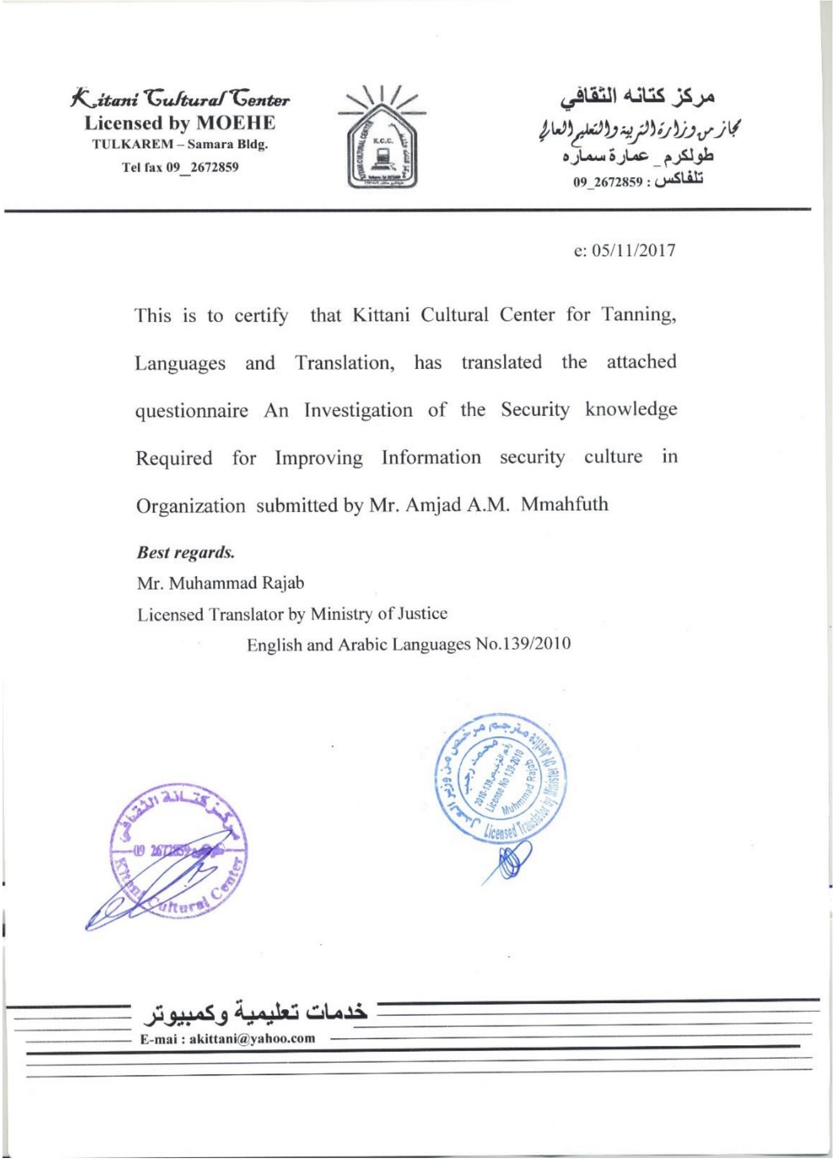
المواقف او الاتجاهات حول المعرفة الامنية(Attitudes (Attitudes towards Security knowledge						
64.	معرفتي بأنواع المعرفة الأمنية المطلوبة في المؤسسة ضروري.					
65.	معرفتي بأنواع المعرفة الأمنية المطلوبة في المؤسسة مفيد.					

66.	موقفي من معرفة أنواع المعرفة الأمنية المطلوبة في المؤسسة لها تأثير ايجابي في الحد من خطر الخروقات الأمنية فيها.					
67.	علمي بأنواع المعرفة الأمنية المطلوبة في مؤسستي هي ذات قيمة.					
68.	موقفي من معرفة أنواع المعرفة الأمنية المطلوبة في المؤسسة لها تأثير ايجابي على حماية أصول المعلومات فيها.					
69.	موقفي من معرفة أنواع المعرفة الأمنية المطلوبة في المؤسسة لها تأثير ايجابي في تقليل مخاطر حوادث أمن المعلومات.					
70.	موقفي من معرفة أنواع المعرفة الأمنية المطلوبة في المؤسسة له تأثير إيجابي على سلوكي الامني داخل المؤسسة.					

شاكر لكم حسن تعاونكم،،

APPENDIX B.

TRANSLATION CERTIFICATE



Kitani Cultural Center
Licensed by MOEHE
TULKAREM – Samara Bldg.
Tel fax 09_2672859

K.C.C.

مركز كتانه الثقافي
مجاز من وزارة التربية والتعليم العالي
طولكرم _ عمارة سماره
تلفاكس : 09_2672859

e: 05/11/2017

This is to certify that Kittani Cultural Center for Tanning, Languages and Translation, has translated the attached questionnaire An Investigation of the Security knowledge Required for Improving Information security culture in Organization submitted by Mr. Amjad A.M. Mmahfuth

Best regards.

Mr. Muhammad Rajab
Licensed Translator by Ministry of Justice
English and Arabic Languages No.139/2010

مركز كتانة الثقافي
09 2672859
Kittani Cultural Center

مترجم مرخص من وزير العدل
محمد رجب
رقم الترخيص 2010-139
License No 139-2010
Muhmmad Rajab
Licensed Translator by Minister of Justice

خدمات تعليمية وكمبيوتر
E-mai : akittani@yahoo.com

APPENDIX C.

ENGLISH QUESTIONNAIRE

Dear participant,

First of all, I would like to thank you for your valuable participation in this research survey, which aims to investigate of the security knowledge required for improving employee security behaviour in organisations as a part of a PhD research in Information Security Management.

Information security culture means that employees have the required values, beliefs and knowledge and behave accordingly in a way that protect the information assets (electronically or not) and to preserve the confidentiality, integrity, reliability and availability of information. For instance, updating antivirus, clear desk policy, strong password, regularly changing the password, not disclose private customer information and so on.

This study is directed at any persons working in the organisation. We assure you that your participation in the survey will be strictly confidential to the research team. Your personal details will be used for research classification purposes only and your identity will be kept anonymous and the name of the organisation will not be disclosed.

Your participation will contribute to obtain accurate results, and to improve the quality of research in information security in Palestinian organisations. Completing the questionnaire may take about 10 minutes. Please try to answer all statements. Each statement can be answered with only a single selection.

Should you have any further queries, please do not hesitate to contact us.

Again, we thank you for your interest and participation in this study.

Yours sincerely,

Amjad Mahfuth

PhD Student,

College of Computer Science & Information Technology
Tenaga National University, Malaysia
amahfouth99@gmail.com

Section A: Personal Information

The following section seeks are general information about you and your organisation. Please answer by ticking (√) in the appropriate bracket below:

Age :

□ Under 25 □ 25 - 35 □ 36 - 45 □ Above 45

Year of experience:

How long have you been working in this organisation?

□ Less than two year □ 2 - 4 Years □ 5 - 10 Years

□ More than

Job Level:

What job level is applied to you?

□ Hospital Management □ Doctor □ Nurse

□ Administartive Staff

Education level:

□ Undergraduate □ Postgraduate

Gender:

□ Male □ Female

Working in IT department) :

Are you working in any area related to IT? e.g. IT department

□ Yes □ No

Education Background in IT:

Was your education in IT related Field?

□ Yes □ No

Work Requirements

Does your work require dealing with any computer or IT technology?

□ Yes □ No

Security Awareness Training:

Have you got any security awareness training?

□ Yes □ No

Section B: Security Knowledge's Construct's :

Please indicate your agreement to the following statements regarding the security knowledge construct’s [1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree]:

Knowledge of Security Threat		**Please tick one**				
		1	**2**	**3**	**4**	**5**
1.	I know the types of harmful threats to information assets.					
2.	I know the negative consequences of an attack on or threat to information assets.					
3.	I understand that security threats (attacks) can occur any time.					
4.	I know the threats and vulnerabilities towards the information assets in my work environment.					
5.	I know about information security threats.					
Knowledge of Organisation Information Security Strategy(information security policy, security requirements, standards and process)						
6.	I know what my organisation’s information security strategy is.					
7.	I know my organisation’s information security strategy helps me protect my organisation’s information assets in my daily work.					
8.	I understand the content of information security strategy elements like policy.					
9.	I know organisation’s information security strategy helps me understand what is expected from me as an employee in terms of safeguarding my organisation’s information assets.					
10.	I know that my organisation has developed information security strategies to address the prevention and detection of threats and to respond to them.					
11.	Employees know information security requirements to protect information.					
12.	I am aware of information security policies related to my job such as the password policy.					
13.	I know that the information security is necessary to protect information in my organisation					
14.	I know that the information security is necessary to increase the confidence that the third parties have in my organisation.					
15.	I know information security practices such as data encryption.					

16.	I know information security practices such as a clear desk policy.					
17.	I know about information security controls (e.g. that I must set up a strong password).					
18.	I know the information security requirements helps me protect the information assets of my organisation.					
Knowledge of Security Technology						
19.	I know the technical tools and controls for information security helps me to preserve information security.					
20.	I know the security technology enables me to help other employees with their technical queries and problems					
21.	I know that the appropriate use of technical controls is vital to achieve information security.					
22.	I know the policy and guidelines for the effective use of information security hardware and software helps me preserve information security and prevent security breaches and threats.					
23.	I know how to use technical measures such as antivirus to ensure information security.					
Knowledge of legislation, regulations, national culture such as act Data Protection Acts, HIPPA, International Standards etc.						
24.	I know the government regulations regarding information security.					
25.	I am aware of relevant government information security related legislation such as copyrights.					
26.	I know the data protection and other relevant legislation and regulations.					
27.	I know the privacy and other relevant legislation and regulations.					
28.	I have clear directives on protecting sensitive and confidential information and applying the related regulations.					
29.	I am aware of the importance of the values of intellectual property and copy right laws.					
30.	I know the process of information security should not conflict with the society ethics and essential value.					
31.	I know the national culture must be taken into account when designing information security policy and guidelines.					
32.	I know the information security measures must comply with international standards.					

Knowledge of Security Responsibility						
33.	I know that information security is my responsibility in the organisation.					
34.	I know that I am responsible for any actions that conflict with information security requirements.					
35.	I know what information security is.					
36.	I know how to report information security incidents.					
37.	I know my role with regards to each security policy.					
38.	I know what to do when I detect a security violation.					
39.	I know what information assets to protect and how I can protect them.					
40.	I know that it is essential to protect information assets to achieve business success.					
41.	I am aware that I should never give my password to somebody else.					
Knowledge of Security Risk						
42.	I know that a weak password represents a security risk.					
43.	I know the risks when opening web links.					
44.	I know the security risks and dangerous to the information assets in my work environment.					
45.	I know the risk when opening e-mails from unknown senders, especially if there is an attachment.					
46.	I know the risk is when sharing passwords between others.					
47.	I know the risk is when giving out confidential information of visit prohibited internet sites.					
48.	I know it is essential to take care when talking about confidential information in public places.					

Section C: Security Behaviour:

Please indicate your agreement to the following statements regarding the security behaviour [1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree]:

Security Behaviour	**Please tick one**				
	1	**2**	**3**	**4**	**5**

49.	I update the anti-virus software regularly.					
50.	I always lock my computer when I leave the desk.					
51.	I ensure that there is no confidential documents left on my desk when I leave the office.					
52.	When I suspect any information threat, I report it straightaway.					
53.	I should act in a way that prevents any threats to information security.					
54.	I share information about threats and vulnerabilities as appropriate.					
55.	I adhere to information security requirements in my organisation.					
56.	I act in a supportive manner to prevent, detect and respond to security incidents.					
57.	I behave carefully when I connecting with email attachments especially from unknown senders					
58.	I can easily ask question and leave comment regarded information security.					
59.	I usually follow my organisations information security strategy in my daily work to protect information assets.					
60.	I have a strong password.					
61.	I do not open email attachments if the content of the email looks suspicious.					
62.	Before reading an email, I will first check if the subject and the sender make sense.					
63.	I never give my personal information (like home/email address, telephone number, etc.) to unknown websites.					

Section D: Attitudes:

Please indicate your agreement to the following statements regarding the attitudes towards security knowledge's [1:Strongly Disagree; 2:Disagree; 3:Neutral; 4:Agree; 5:Strongly Agree]:

Attitudes (Attitudes towards Security knowledge)		**Please tick one**				
		1	**2**	**3**	**4**	**5**
64.	Knowing the types of security knowledge required in my organisation is necessary.					
65.	Knowing the types of security knowledge required in my organisation is beneficial.					

66.	My Attitude towards understanding the types of security knowledge required will have a positive effect on mitigating the risk of security breaches.					
67.	Knowing the types of security knowledge required in my organisation is a valuable.					
68.	My Attitude towards understanding the types of security knowledge required will have a positive effect on safeguarding the organisation's information assets.					
69.	My Attitude towards understanding the types of security knowledge required will have a positive effect on decreasing the risk of information security incidents.					
70.	My Attitude towards understanding the types of security knowledge required will have a positive effect on my security behaviour in my organisations.					

Thank You for Your Co-operation

APPENDIX D.

INTERVIEW GUIDE

Organisation name: ______________________

Position? _____________________________

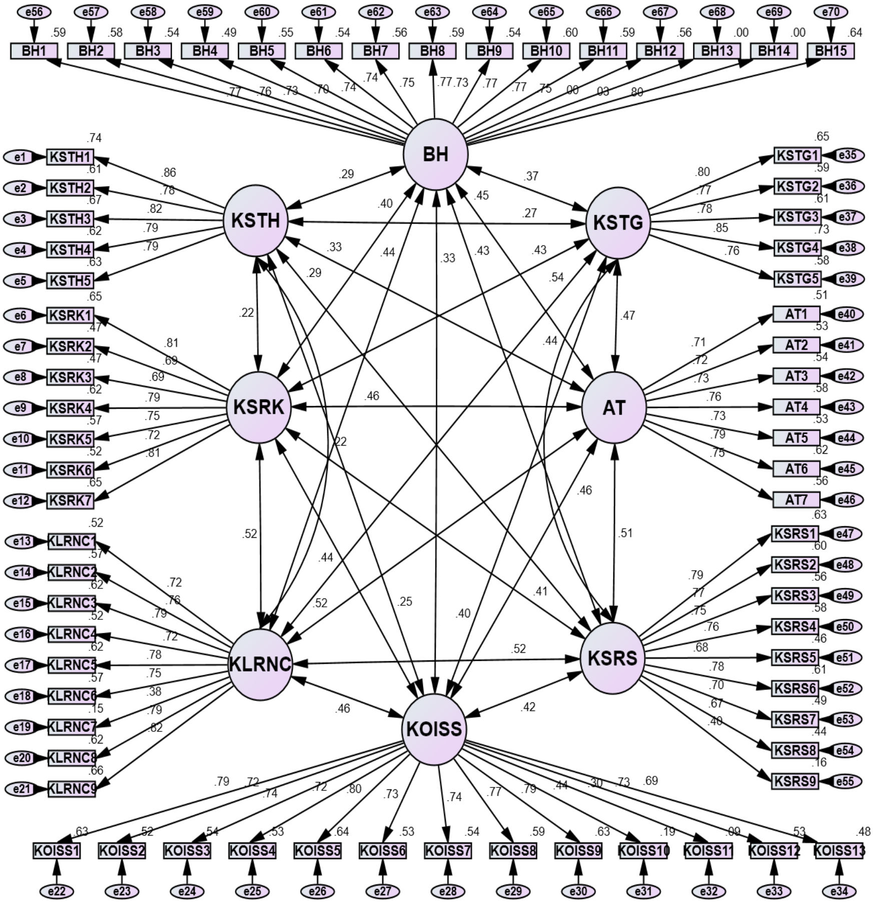
How long have you been working in your organisation

□Less than a year □2 -4 □5-10 □more than 10 years

1. What are the security awareness training program in the organisation for the employee?
2. Organisation employees knowledge about security threat will help to influence their security behaviour when they interacting with organisation assets? Please explain.
3. Providing security awareness training about organisation information security strategy will help to influence their security behaviour in the organisation? Please elaborate.
4. Employees' knowledge about security technology will help to influence their security behaviour in the organisation? Please explain.
5. Do you think the employees' knowledge of legislation, regulation and national culture will help to influence their security behaviour in the organisation? Please explain.
6. Employees' knowledge about security responsibility will help to influence their security behaviour in the organisation? Please explain.
7. Do you think the employee's knowledge of security risk will help to influence their security behaviour in the organisation? Please explain.
8. Are those security knowledge constructs help to improve the employee security behaviour in organisations? Please explain.
9. How these security knowledge constructs help to reduce the internal security incidents posed by the employee?

APPENDIX E.

ALL EXOGENOUS AND ENDOGENOUS VARIABLES TOGETHER WITH THEIR RELATIVE ESTIMATION ERRORS



Absolute Fit Indices
df = 2317
Chi Square = 4328.964

p-value = .000
GFI = .755
AGFI = .737
RMSEA = .049

Incremental Fit Indices
CFI = .872
TLI = .867
IFI = .873

Parsimonious Fit Index
NORMEDCHISQ = 1.868

APPENDIX F.

OBSERVATIONS FARTHEST FROM THE CENTROID (MAHALANOBIS DISTANCE)

Number of variables in the model = 148

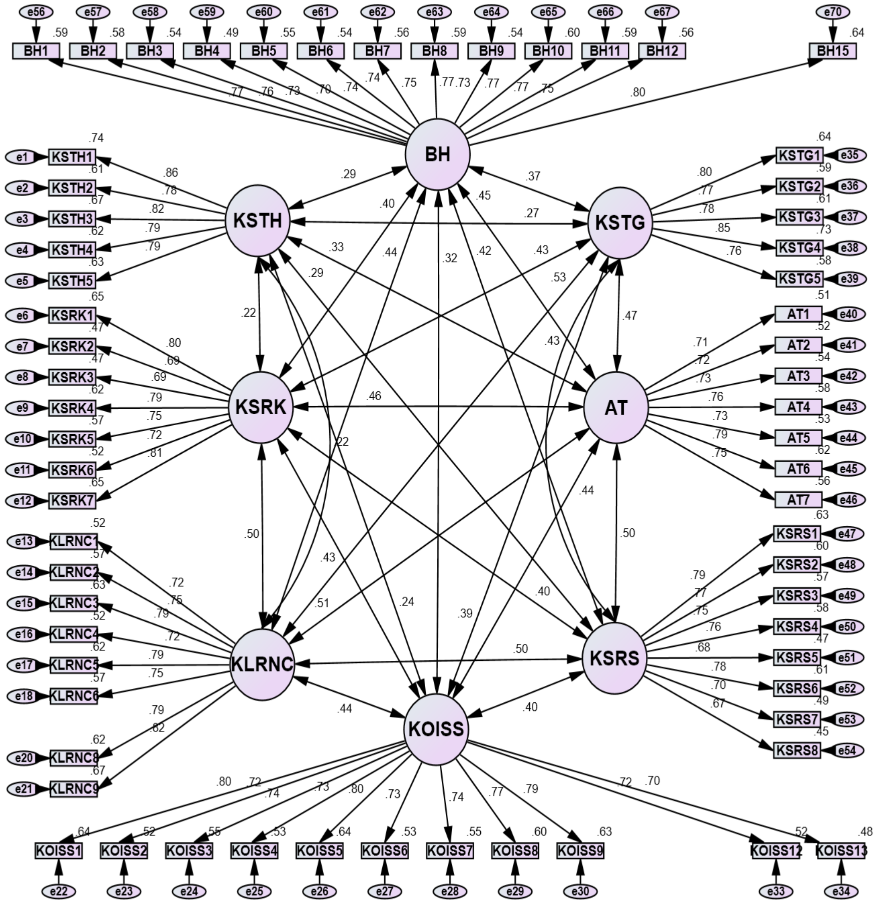
Max (D^2) / (no. variables) = 103.449 / 148 = 0.699 which is < 3.5 → No Multivariate Outliers

Observation number	Mahalanobis d-squared	p1	p2
250	103.449	.006	.876
306	103.086	.006	.653
217	100.851	.009	.651
41	99.934	.011	.555
110	97.618	.016	.700
20	96.008	.021	.781
115	94.728	.026	.836
179	94.635	.027	.746
349	94.464	.027	.656
86	93.788	.030	.662
200	93.703	.031	.559
202	93.561	.032	.468
58	92.591	.037	.566
14	92.234	.039	.536
331	91.141	.046	.682
283	90.189	.053	.791
201	89.855	.055	.781
91	89.845	.055	.706
180	89.538	.058	.694

Observation number	Mahalanobis d-squared	p1	p2
130	89.387	.059	.647

APPENDIX G.

SECOND ITERATION OF CFA WITH 64 REMAINING ITEMS



Absolute Fit Indices
df = 1924
Chi Square = 3120.271

p-value = .000
GFI = .796
AGFI = .779
RMSEA = .042

Incremental Fit Indices
CFI = .919
TLI = .915
IFI = .919

Parsimonious Fit Index
NORMEDCHISQ = 1.622