AN INVESTIGATION OF HEALTH INFORMATION SYSTEM SECURITY POLICIES COMPLIANCE BEHAVIOUR

NORSHIMA HUMAIDI

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

UNIVERSITY OF MALAYA

KUALA LUMPUR

2016

AN INVESTIGATION OF HEALTH INFORMATION SYSTEM SECURITY POLICIES COMPLIANCE BEHAVIOUR

NORSHIMA HUMAIDI

THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

UNIVERSITY OF MALAYA

KUALA LUMPUR

2016

UNIVERSITY OF MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: (I.C/Passport No:)

Registration/Matric No:

Name of Degree:

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"):

Field of Study:

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;

(2) This Work is original;

(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;

(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;

(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;

(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate’s Signature   Date:

Subscribed and solemnly declared before,

Witness’s Signature   Date:

Name:

Designation:

ABSTRACT

Health Information System (HIS) has a higher degree of vulnerability towards threats of information security such as unauthorized access, use, disclosure, disruption, modification or destruction and duplication of passwords. Human error is a major security threat to information system's security and this is usually constituted by carelessness, ignorance and failure to comply with organization information security policies (ISPs). Using health professionals' data from a quantitative survey, Partial Least Squares-Structural Equation Modelling (PLS-SEM) analysis was used to determine the factors that affect users' compliance behaviour towards HIS security policies and HIS prototype was developed based on the significant factors. In addition, insights gained from interviews with a small sub-sample of health professionals, who were interviewed during prototype testing, were used to further examine compliance behaviour among health professionals. This study introduced a new human behaviour model, namely, Health Information System Security Policies Compliance (HISSPC) model by positing the mediation effect of factors in Health Belief Model (HBM) (Perceived Severity, Perceived Susceptibility and Perceived Benefit) and Self-Efficacy, while HIS experience as a moderating variable in the context of security management, which is largely unknown among scholars to investigate the relationship between management support and HIS security policies compliance behaviour among Malaysian health professionals. Theory of planned behavior (TPB) is adapted to measure user's perception towards management support. Additionally, trust factor is also added in the HISSPC model to increase the understanding of human behavior in complying with HIS security policies.

Exploratory factor analysis (EFA) revealed seven-factors: Management Support, Perceived Severity, Perceived Susceptibility, Perceived Benefit, Perceived Barrier, Self-

Efficacy and Trust. Confirmatory factor analysis (CFA) testing shows that all the measurement items of each constructs were adequate in their validity individually based on their factor loading value. Moreover, each constructs are valid based on their parameter estimates and statistical significance. The quantitative research findings show that Management Support strongly influences Self-Efficacy compared to other information security awareness factors. Meanwhile, Trust was the most significant factor influencing HIS security policies compliance behaviour while Perceived Susceptibility did not appear significant. Perceived Severity, Perceived Benefit and Self-Efficacy were found to mediate the effect of Management Support on HIS security policies compliance behaviour. PLS-SEM has shown that Management Support is significant for low experience users while Perceived Susceptibility strongly influences high experience users to comply with HIS security policies.

The qualitative research findings thru prototype testing found that all the factors in HISSPC model contributes to user's compliance behaviour towards ISPs. In addition, most of the respondents are satisfied with the proposed system.

This study utilizes the multidimensional approach of human-technical interactions to evaluate the relationship between the integrated social-technical values and actions of compliance towards HIS security policies among selected Malaysian health professionals. The study believes that the research findings can contribute to human behaviour in IS studies and are particularly beneficial to policy makers in improving organizations' strategic plans in information security, especially in healthcare sectors. Most organizations spend time and resources to provide and establish strategic plans of information security; however, if employees are not willing to comply and practice information security behaviour appropriately, then these efforts are in vain.

ABSTRAK

Sistem Maklumat Kesihatan (HIS) mempunyai tahap kelemahan yang tinggi terhadap ancaman keselamatan maklumat seperti capaian yang tidak dibenarkan, penggunaan, pendedahan, gangguan, pengubahsuaian atau pemusnahan dan pertindihan kata laluan. Kesilapan manusia adalah ancaman keselamatan utama kepada keselamatan maklumat dan ini biasanya dibentuk oleh kecuaian, kejahilan dan kegagalan untuk mematuhi dasar-dasar keselamatan maklumat organisasi. Menggunakan data professional kesihatan daripada kajian kuantitatif, analisis Partial Least Squares-Structural Equation Modelling (PLS-SEM) telah digunakan untuk menentukan faktor-faktor yang memberi kesan gelagat kepatuhan pengguna terhadap dasar keselamatan HIS dan prototaip HIS telah dibangunkan berdasarkan faktor penting yang didapati. Di samping itu, kefahaman yang diperoleh daripada temubual dengan sampel kecil daripada profesional kesihatan yang telah ditemuramah semasa ujian prototaip, telah digunakan untuk mengkaji lagi gelagat kepatuhan di kalangan profesional kesihatan. Kajian ini memperkenalkan model tingkah laku manusia yang baru, iaitu, model Dasar Kesihatan Sistem Maklumat Pematuhan Keselamatan (HISSPC) dengan meletakkan pengantaraan faktor dalam Health Belief Model (HBM) (Tanggapan Kerentanan, Tanggapan Keterukan, dan Tanggapan Manfaat) dan Keberkesanan-Diri, manakala pengalaman menggunakan HIS sebagai pembolehubah sederhana dalam konteks pengurusan keselamatan, yang sebahagian besarnya tidak diketahui di kalangan penyelidik untuk mengkaji hubungan di antara sokongan pengurusan dan tingkah laku dasar keselamatan pematuhan di kalangan profesional kesihatan Malaysia. Theory of Planned Behaviour (TPB) digunakan untuk mengukur persepsi pengguna ke arah sokongan pengurusan. Selain itu, faktor kepercayaan juga ditambah didalam model HISSPC untuk meningkatkan pemahaman tentang tingkah laku manusia dalam mematuhi dasar-dasar keselamatan HIS.

Analisis faktor penerokaan (EFA) mendedahkan tujuh faktor: Sokongan Pengurusan, Tanggapan Keterukan, Tanggapan Kerentanan, Tanggapan Manfaat, Tanggapan Penyekat, Keberkesanan-Diri dan Kepercayaan. Ujian analisis faktor pengesahan (CFA) menunjukkan bahawa semua item pengukuran setiap konstruk adalah mencukupi dalam pengesahan secara individu berdasarkan nilai faktor muatan mereka. Selain daripada itu, setiap konstruk juga adalah sah berdasarkan anggaran parameter dan kepentingan statistic. Dapatan kajian kuantitatif menunjukkan bahawa Sokongan Pengurusan mempengaruhi Keberkesanan-Diri berbanding dengan faktor-faktor kesedaran keselamatan maklumat yang lain. Sementara itu, Kepercayaan adalah faktor yang paling penting mempengaruhi dasar keselamatan gelagat kepatuhan HIS manakala Tanggapan Kerentanan tidak kelihatan ketara. Tanggapan Keterukan, Tanggapan Manfaat dan Keberkesanan-Diri didapati memberi kesan pengantara antara Sokongan Pengurusan dan dasar keselamatan gelagat kepatuhan HIS. PLS-SEM menunjukkan bahawa Sokongan Pengurusan adalah penting untuk pengguna yang kurang berpengalaman manakala Tanggapan Kerentanan mempengaruhi pengguna yang berpengalaman untuk mematuhi dasar-dasar keselamatan HIS.

Dapatan kajian kualitatif melalui ujian prototaip mengesahkan bahawa semua faktor dalam model HISSPC menyumbang kepada gelagat kepatuhan pengguna ke arah dasar-dasar keselamatan maklumat. Selain itu, sebahagian besar daripada responden berpuas hati dengan sistem yang dibangunkan.

Kajian ini menggunakan pendekatan pelbagai dimensi interaksi teknikal-manusia melalui teori pelbagai disiplin untuk menilai hubungan di antara nilai-nilai sosial-teknikal bersepadu dan tindakan pematuhan terhadap dasar keselamatan HIS di kalangan profesional kesihatan Malaysia di hospital yang terpilih. Kajian ini percaya bahawa hasil penyelidikan menyumbang kepada kajian tingkah laku manusia dan sistem maklumat adalah memberi manfaat kepada pembuat dasar dalam meningkatkan pelan strategik organisasi dalam keselamatan maklumat, terutamanya dalam sektor penjagaan kesihatan. Kebanyakan organisasi menghabiskan masa dan sumber untuk menyediakan dan mewujudkan pelan strategik keselamatan maklumat; walau bagaimanapun, jika

pekerja tidak bersedia untuk mematuhi dan mengamalkan tingkah laku maklumat keselamatan dengan sewajarnya, maka usaha-usaha ini adalah sia-sia.

ACKNOWLEDGEMENTS

Assalamualaikum WBT, praise to Allah the Almighty for giving my health and strength to complete Ph.D research. Firstly, thanks to my supervisor and co-supervisor, Dr. Vimala A/P Balakrishnan and Professor Dr. Abrizah Binti Abdullah for the support, insightful, suggestions and endless patience towards the end. Without help and commitment, this study cannot be completed within specified time.

I would also express my gratitude to my husband Mohammad Syazwan Bin Mohd, my lovely family and friends for their support, guidance and encouragement throughout every phase of the Ph.D journey which help making this research possible.

I also like to thank individuals who involved directly and indirectly for the advice and assistance in preparing this research:

- Hospital Director of Hospital Selayang, Hospital Serdang and Hospital Sungai Buloh
- Clinical Research Officer of Hospital Selayang, Hospital Serdang and Hospital Sungai Buloh
- Nurse Farida Binti Mohamed Jamion (Hospital Selayang)
- Office Clerk at Pharmacy Department, Specialist Department and Health Record Department (Hospital Selayang, Hospital Serdang and Hospital Sungai Buloh)

Last but not least, my gratitude is for all those who helped in collecting data and also the peoplewho agreed to take part in the research.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

HISSPC	:	Health Information System Security Policies Compliance
HIS	:	Health Information System
ISPs	:	Information Security Policies
MOH	:	Ministry of Health
MAMPU	:	Malaysian Administrative Modernization and Management Planning Unit
IT	:	Information Technology
IS	:	Information System
PLS-SEM	:	Partial Least Squares-Structural Equation Modelling
EFA	:	Exploratory Factor Analysis
CFA	:	Confirmatory Factor Analysis
EFA	:	Exploratory Factor Analysis
CMB	:	Common Method Bias
HOD	:	Head of Department

LIST OF APPENDICES

CHAPTER 1: INTRODUCTION

1.1 Background of the Study

The waves of evolutionary reality among heterogeneous information and communication technologies have expanded multi-dimensional spaces of health informatics (HI) based on *good to have* discipline. Positive signals of health care have resulted in dynamic changes in virtual health communications (Haux, 2010) and has paved the way for the emergence of health information systems (HIS) in the early 1990s (Sezgin & Yildirim, 2014). The increasing use of HIS in various fields of healthcare services have expanded the degree of accessibility and capacity (Nah, Siau, & Sheng, 2005). This has assisted health professionals in the arrangement of schedule and maintenance of daily operations in the health institutions (Haux, 2006). The terms of "Health Information System" and "Hospital Information System" differ in terms of definitions as the latter is the subset of former. The former is more applicable to general audiences whereas the latter suits to specific users (Aniza Ismail et al., 2010).

The rapid growth of Information and Communication Technology (ICT) has allowed the Ministry of Health (MOH) to embark on implementing HIS in several local hospitals, especially those that are located in the Klang Valley, such as Selayang Hospital, Sungai Buloh Hospital, Serdang Hospital, and Universiti Kebangsaan Malaysia Medical Centre (UKMMC) (Aniza Ismail et al., 2010). HIS has been implemented in health institutions with several sub-systems integrated that are designed to manage the administrative, financial, and clinical aspects of hospitals with the aim of providing the best services to patients while managing hospital records effectively (Nurul Izzatty Ismail, Nor Hazana Abdullah, Alina Shamsudin, & Nik Azliza Nik

Ariffin, 2013). Moreover, the system provides more cost-effective health care and support information in the medical domain. It also brings many benefits to health institutions, such as reduced data processing time (Nurul Izzatty Ismail et al., 2013; Nurul Izzatty Ismail & Nor Hazana Abdullah, 2012).

Although HIS is an example of innovative product towards effective healthcare delivery, it has a higher degree of vulnerability towards the threats of information security such as unauthorized access, use, disclosure, disruption, modification or destruction and duplication of passwords. This could be due to the greater openness of multi-connectedness between heterogeneous stakeholders within the networks. Information security threat is defined as undesirable incidents that can cause different types of damage, which might lead to the loss of an organization’s finances or reputation (Alhabeeb, Almuhaideb, Le, & Srinivasan, 2010). The information security threat is a major issue in online banking and e-commerce, and today it has also progressed to health institutions (Fernández-Alemán et al., 2015; Gathan Narayana Samy, Rabiah Ahmad, & Zuraini Ismail, 2009).

Furthermore, health information is extremely sensitive, and high protection is therefore required. This information needs to be protected while being transmitted, stored, and processed (Fernández-Alemán et al., 2015; Dlamini, Eloff, & Eloff, 2008). Therefore, information security is required to protect health data from being stolen or harmed. Information security is defined as the protection of information systems from unauthorized access and information threat (Tamjidyamcholo, Bin Baba, Tamjid, & Gholipour, 2013; Cavalli, Mattasoglio, Pinciroli, & Spaggiori, 2004). Information security is one of the important elements that should be considered in the development of an information system (IS). Many organizations with IS have implemented advanced security technologies, such as smart card and biometrics (Kreicberge, 2010). However, these technologies cannot promise effective information system security if the information security behaviour of employees in the organization is unacceptable. The employees or the users of IS are actually the primary and the most critical line of defence (Eminağaoğlu, Uçar, & Eren, 2009). This notion is also supported by other studies that state that employees are the key factor to either the success or failure of information system security in any organization (Abdul Rahman Ahlan, Yusri Arshad, & Muharman Lubis, 2011; Bulgurcu, Cavusoglu, & Benbasat, 2009).

According to Ganthan Narayana Samy, Rabiah Ahmad, & Zuraini Ismail (2010), the setbacks of information security system are strongly linked to human actions than physical failures. This can be divided into unintended and intended human failures (Safa, Von Solms, & Furnell, 2016). Intended actions are caused by employees and designers of Human-Computer Interaction (HCI) through privileged access to the embedded facilities within an organization (Colwill, 2009; Schneier, 2005). Unintended lines are due to the complexity and unfriendly nature of security mechanism within HIS (Safa et al., 2016; Renaud, 2012; Liginlal, Sim, & Khansa, 2009; Vroom & von Solms, 2004).

Insecurity could reduce trust and this could influence non-compliance behaviour on information security policies (ISPs). The choice of compliance among employees depends on individual goals, perceptions of employees and organizational context (Weirich & Sasse, 2001; Adams & Sasse, 1999). Protective security guidelines are recognized as an *intellectual saviour* towards growing trends of threats (Knapp, Franklin Morris Jr, Marshall, & Byrd, 2009). Management of compliance behaviour towards security policies among health professionals is considered to be a great challenge as it is closely connected to the complete design of security models (Eric & Goetz, 2007). It deals with the combined evaluation of technical and human factors (Al-

Omari, El-Gayar, & Deokar, 2012b; Eminağaoğlu et al., 2009) to maintain a win-win paradigm of system. Therefore, the top management should consider and invest not only in the technical part of the system, but also in the human resources (Da Veiga & Martins, 2015). This is also argued by recent study, whereby the technology cannot solely gurantee a secure environment for organization’s information; information security behaviour among employees should be taken into consideration, besides the technological aspects (Safa et al., 2016).

1.2 Definitions and Terms

The following definitions are utilized in this study:

Health Information System

Minister of Health (MOH) in Malaysia introduced Health Information System (HIS) to integrate several information system (IS) that consist of one central main hospital information system, which covers basic Enterprise Resource Planning (ERP)-like functionality, such as patient registration, billing, documentation, inventory, and other functions that require corporate involvement (Nurul Izzatty Ismail et al., 2013; Luethi & Knolmayer, 2009;). Additionally, those systems may include or are connected to ancillary systems, such as laboratory, pharmacy, and X-ray components.

Information Security Threat

An information security threat is a threat that can cause damage to an organization’s data (Akhunzada et al., 2015; Metalidou et al., 2014). In addition, an organization might experience loss in terms of financial or reputation, or both when an information security threat cannot be controlled (Saathoff, Nold, & Holstege, 2013; Gathan Narayana Samy et al., 2010). Information security threats can be divided into two: external and internal threats. External threats are caused by an outsider (Sharma & Sefchek, 2007), which can be easily controlled using security technologies such as firewalls (Colwill, 2009). However, this current study only focuses on the internal threat, which is defined as a threat caused by insiders (employee, ex-employee, partner or client) who misuse the access given by the organization in a negative way, e.g. user errors, user negligence and deliberate acts against the company (Kreicberge, 2010; Liu, Ji, & Mookerjee, 2009). Therefore, to protect the organization's information from being stolen or harmed, information security is required.

Information Security

An information security plays an important role in protecting health data from theft and abuse. Information security in health institutions is used to protect health data from unauthorized access, use, disclosure, disruption, modification or destruction (Mahmood Hussain Shah, Hamid Reza Peikari, & Norjaya M. Yasin, 2014; Tesema, Medlin, & Abraham, 2010). According to Brady (2010), information security is a program that allows an organization to protect a continuously interconnected environment from emerging weaknesses, vulnerabilities, attacks, threats, and incidents.

Information Security Awareness

Information security awareness refers to users' understanding towards the importance of information security and their responsibility to practice computer security behaviours to protect an organization's data (Shaw, Chen, & Harris, 2009; Rezgui & Marks, 2008). For example, users who are aware of information security understand that the consequences of their pro-security actions would be beneficial to them and/or to their organization Bulgurcu et al. (2009). This element is important because if the employees are aware of the information security issues, they will be more cautious, more responsible, and will handle their tasks properly.

Management support

Management support explains the commitment from the top management to protect information as a critical security component (Da Veiga & Eloff, 2010). Management support is a critical element that can affect an employee's compliance behaviour towards information security (Renaud, 2012). Studies have explained that management support has a strong relationship to the success of IS implementation (Brady, 2010). The management should show their security support by spreading the security message to all employees in the organization (Vance, Siponen, & Pahnila, 2012), and ensuring that all employees utilise the IS and security tools effectively (Gathan Narayana Samy et al., 2010; Rhee, Kim, & Ryu, 2009).

Information Security Policies

One of the approaches to prevent an internal threat is by implementing information security policies (ISPs). The ISPs are a set of rules and procedures that help to define recommended information security levels in the organization that employees should follow (Yildirim, Akalp, Aytac, & Bayram, 2011). These policies highlight the importance of information security aspects, such as how to protect valuable information from an information security threat (Knapp et al., 2009), and help to reduce the number of security incidents in an organization (Kruger & Kearney, 2006).

Information System (IS) Security Compliance Behaviour

An information security compliance behaviour is described as behaviours which do not violate organization ISPs (Guo, 2012) and those that adhere to a set of core information security activities as recommended by the organization (Padayachee, 2012). The current study believes that if the users' behaviour towards information security is acceptable, such as being responsible while handling the organization's data, and complies with the organization's ISPs, security incidents can be decreased and the effectiveness of IS security can be increased.

1.3 Statement of the Problem

The most stimulating issue in information system (IS) security is human behaviour and "*dealing with them it is perhaps one of the biggest challenges that organizations face today"* (Akhunzada et al., 2015, p. 45). One of the most critical factors affecting IS security is related to user behaviour (Safa et al., 2016; Da Veiga &

Martins, 2015; Fernández-Alemán et al., 2015), that is, human errors (Parsons et al., 2014; Colwill, 2009), which are classified into two categories: human slips and human mistakes. According to Liginlal et al. (2009), human slips occur as an outcome of the incorrect execution of a correct action sequence, which usually happens because of human carelessness, such as inadequate written communication (prescriptions, documentation, transcription) (Keers, Williams, Cooke, & Ashcroft, 2013). Meanwhile, human mistakes occur as an outcome of the correct execution of an incorrect action sequence, i.e., wrong decisions executed correctly because of human ignorance, and failure to comply with an organization's security policies (Boujettif & Yongge, 2010; Gathan Narayana Samy et al., 2010), for an example, the behaviour such as sharing password with other people.

Human error is a major threat to IS security (Al-Omari, El-Gayar, & Deokar, 2012a; Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; Seppo, Mikko, & Adam, 2007). Although many organizations have implemented the latest security technologies, such as biometrics, smartcards, and encryption (Kreicberga, 2010), user's behaviour towards information security is still weak, and thus, issues relating to information securities have increased (Park, Ruighaver, & Ahamad, 2010). This is because the technologies cannot promise effective IS security if the information security behaviour of employees in the organization is unacceptable. Most of the previous studies have argued that technology is not the problem, and that user's behaviour towards information security is the main issue (Barlow, Warkentin, Ormond, & Dennis, 2013; Warkentin, Johnston, & Shropshire, 2011). This is also supported by other studies whereby many security incidents were caused by employees in the organizations (Al-Omari, Deokar, El-Gayar, Walters, & Aleassa, 2013; Ifinedo, 2012; Kreicberga, 2010; Sun, Ahluwalia, & Koong, 2011).

Organizations might lose millions of dollars due to security incidents because of employee negligence, and non-compliance with the organization’s ISPs, such as not creating strong passwords, leaving the computers without any protection, and being irresponsible while handling organizational data and information (Akhunzada et al., 2015; Herath & Rao, 2009a).

HIS security threats, such as human error have increased significantly in recent years (Safa et al., 2016; Akhunzada et al., 2015; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Barlow et al., 2013; Al-Omari et al., 2013, 2012a). Many previous studies have reported that many organizations have faced security incidents and that the statistics for security failures due to user’s behaviour is 80% and are continuing to increase, even though organizations have invested more in security technology-based solutions (Da Veiga & Martins, 2015; Safa et al., 2015; Boujettif & Yongge, 2010; Bulgurcu et al., 2009). Moreover, global Internet security reported that, in 2012, the healthcare sector had the largest percentage of security incidences, which was 36% compared to other sectors (Symantec, 2013). In 2013, more than 7 millions health information breached were reported (Redspin, 2013). These incidences can be very costly to any organization (Goel & Shawky, 2009), and in 2012, the statistics for financial losses from internal attacks alone was 60% (Renaud, 2012).

Studies related to information security are many; however, to the best of our knowledge, studies conducted to assess users’ information security compliance behaviour in the health institutions (Noor Hafizah Hassan & Zuraini Ismail, 2012; Suhaila Samsuri, Rabiah Ahmad, & Zuraini Ismail, 2011) are somewhat scarce, especially in Malaysia. A report regarding unethical doctors who violated the confidentiality of employees’ medical records has also surfaced in Malaysia (The Star, 2009). Furthermore, Gathan Narayana Samy et al. (2009) found that human error is one of the major internal security threats that exists in the healthcare sector in Malaysia. In addition, an information security survey done by Unisys Malaysia (2013) stated that 63% of Malaysian respondents said that they were concerned about data breaches in the healthcare sector. Hence, the practice of information security behaviour by health professionals is essential because it can reduce information security threats, and thus increases the effectiveness of HIS security.

Information security threats exist in the healthcare sector due to the lack of security awareness among employees, poor security skills, poor security monitoring and enforcement as well as inappropriate information security behaviour (Safa et al., 2016; Da Veiga & Martins, 2015; Safa et al., 2015; Liginlal, Sim, Khansa & Paul, 2012; Gathan Narayana Samy et al., 2009). Employees who have adequate knowledge in information security and who understand the consequences of their pro-security actions would be more careful in handling organizational data and information (Parsons et al., 2014). Employees must also develop their own self-awareness towards the issue. This can be more effective if the management implements proper ISPs and provides effective information security training and education (Al-Omari et al., 2013; Barlow et al., 2013). Therefore, information security threats due to human error cannot be underestimated as they impose great risks to health institutions if not managed and controlled accordingly and frequently (Abdul Rahman Ahlan et al., 2011). Security threats are a serious issue in all sectors, especially the healthcare sector.

Furthermore, in healthcare environments, health professionals are HIS users and they must give full commitment when dealing with health data (Brady, 2010), especially when the data can be accessed through a network that is vulnerable and poses a risk to the security of the healthcare data (van Deursen, Buchanan, & Duff, 2013). Possible security risks, among others, include staff sharing passwords to access health data, leaving the computers without logging out and staff emailing health data to the wrong addressee, thus disclosing patient data to an unauthorized user. Therefore, trust in the information security implemented in the health institution plays an important role in influencing security compliance behaviour among health professionals, so that security incidents can be reduced.

There are a few human behaviour theories adapted by previous literature in the area of information security such as Theory of Planned Behaviour (TPB) (Ifinedo, 2012), Health Belief Model (HBM) (Ng, Atreyi, & Yunjie, 2009), Protection Motivation Theory (PMT) (Vance et al., 2012), and Deterrence Theory (Cheng, Li, Li, Holm, & Zhai, 2013), among others. However, to the best of our knowledge, lack of human behaviour theories utilise the combination of human-technical factors (Safa et al., 2015; Shropshire, Warkentin, & Sharma, 2015). Most of the theories do not focus much on the mediation effect of information security awareness and self-efficacy, particularly in respect to the relationship between management support and user compliance behaviour towards ISPs. Additionally, other potential factors such as trust and security barriers in relation to information security behaviour were not explored much. Trust on organization ISPs can improve compliancy, while barrier towards compliancy with ISPs causes non-compliant behaviour among employees (Brady, 2011). Lack of proper knowledge of information security as well as confidence and skills in practising information security mechanisms, employees will not be able to utilize ISPs appropriately. Bearing this issue in mind, the current study was undertaken to investigate health professional’s compliance behaviour towards HIS security policies using a new research framework. The objectives of the current study are as follows as listed in section 1.4.

1.4 Research Objectives (RO) and Research Questions (RQ)

As mentioned in the previous section, human error is one of the major security issues in the organization especially in health care sector (Fernández-Alemán et al., 2015; Gathan Narayana Samy et al., 2009). It is believed that this issue can be reduced through involvement of the management by monitoring their employees' security behaviour and implementing security training to increase security awareness and security skills among employees (Safa et al., 2016; Safa et al., 2015; Shropshire et al., 2015). Moreover, the management should also inculcate the level of confidence and trust among employees towards security policies that are implemented in the organization, because a lack of trust towards an organization's security policies can lead to negligence behaviour (Jiang & Probst, 2015; Brady, 2010; Al-Salihy, Ann, & Sures, 2003).

To the best of our knowledge, lack of theories and models (Fernández-Alemán et al., 2015; Fernández-Alemán, Señor, Lozoya, & Toval, 2013; Brady, 2011) that have focused on the management roles, human trust and information security awareness among health professionals in preventing human error issues in the Malaysian healthcare sector. Besides technological aspects, user's information security behaviour plays an important role in providing a secure environment (Safa et al. 2015). Users sometimes faced difficulties in security implementation, and misinterpret, mistrust or override the security (Cox, 2012). This will cause negligence behaviour among users to adopt appropriate information security behaviour (Shropshire et al., 2015). In an effort to increase the effectiveness of HIS security in Malaysian health care sector, this study aim to examine HIS users' compliance behaviour towards ISPs by focusing on managerial aspects and human factors. Therefore, the following research objectives (RO) and research questions (RQ) have been constructed.

RO1: To develop a Health Information System Security Policies Compliance (HISSPC) model.

In order to achieve RO1, the current study constructed the following research question.

RQ1: What are the factors that can be used to develop the HISSPC model?

Through the development of the research model, this study adapted multidisciplinary of human behavioural theories to evaluate health professional's compliance behaviour towards HIS security policies. This was done by reviewing human behaviour theories and models that were developed by previous researchers. Based on the reviews, several human-technical factors have been identified.

The identified factors have been used to construct the Health Information System Security Policies Compliance (HISSPC) conceptual model. The HISSPC model is relied upon to address the antecedents of human compliance behaviour from management, technical and human aspects. A significant number of previous studies have discussed the behaviour towards information security in other areas, such as the banking industry (Huang, Patrick Rau, Salvendy, Gao, & Zhou, 2011; Roy Sarkar, 2010; Siponen, Pahnila, & Mahmood, 2010). However, to the best of our knowledge, only a few were conducted to assess the HIS security policies compliance behaviour and the mediation effect of information security awareness and self-efficacy, particularly concerning the relationship between management support and users' compliance behaviour towards ISPs (Brady, 2011; Suhaila Samsuri et al., 2011).

In addition, studies on other factors, such as trust and security barriers in relation to information security behaviour, were hardly explored. Trust in an organization's ISPs can improve compliancy while barriers towards compliancy with ISPs cause non-compliant behaviour among employees (Brady, 2011). A lack of proper knowledge concerning information security as well as confidence and skills in practising information security mechanisms, will lead to employees being unable to utilize ISPs appropriately. Therefore, this study was motivated to investigate the impact of the indicated factors on the compliance behaviour of users towards ISPs related with HIS uses.

Bearing in mind the above issues, RO2 was developed, as explained below.

RO2: To determine the relationships between the factors in the HISSPC model and users' compliance behaviour towards Health Information System (HIS) security policies.

This study determines the direct and indirect effects of factors in the HISSPC model and user-compliance behaviour towards ISPs among HIS users. Additionally, this study also describes the moderating effect of HIS experience among healthcare professionals as a supplementary study whereby two types of HIS users were researched based on their experience using HIS. This supplementary study was conducted to test the moderating effect of HIS experience between HISSPC factors and users' compliance behaviour towards HIS security policies. Applying multi-group analysis, the research model is further separated into two models (High Experience Model and Low Experience Model). The following RQ was developed to achieve RO2.

RQ2: What is the relationship between the factors in the HISSPC model and users' compliance behaviour towards HIS security policies?

In order to answer RQ2, several sub-questions were constructed:

RQ2.1: To what extent does the indicated factor in the HISSPC model influence users' compliance behaviour towards HIS security policies?

RQ2.2: To what extent does the intervening factor in the HISSPC model influence users' compliance behaviour towards HIS security policies?

RQ2.3: To what extent does the HIS experience moderate the influence of the factors in the HISSPC model on users' compliance behaviour towards HIS security policies?

This study proposes twelve research hypotheses to answer all the RQs above, which are discussed in the last section of Chapter 2. The PLS-SEM analysis was used to test each of the research hypotheses. According to Karjalainen (2011), if the study focused solely on theory validation, it might present a biased viewpoint of the area of interest. Therefore, the current study incorporates both the quantitative and qualitative research methods for data gathering and analysis.

First, findings from the PLS-SEM analysis were used to identify new requirements of the HIS module for prototype development. *Next,* the prototype was developed to gather in-depth quantitative results from health professionals who agreed to participate in a one-to-one experimental testing process. The participants were interviewed at the end of the testing period with the aim of understanding the compliance behaviour among HIS users towards ISPs based on their experience using the proposed prototype. In doing so, RO3 was constructed:

RO3: To evaluate the HISSPC model using a HIS prototype.

Overwhelmingly, previous studies of security incidents reported by many organizations show an increasing statistical trend in security failures due to user behaviour, despite large investments in security based technology solutions (Da Veiga & Martins, 2015; Safa et al., 2015; Boujettif & Yongge, 2010; Bulgurcu et al., 2009). According to Box and Pottas (2013), these security incidents can be controlled through security measures operating within an information security management system. However, it is imperative for the user to practice proper information security behaviour for these measures to work. Previous studies also argued that many security incidents in the organization are caused by human error due to poor security behaviour by employees (Safa et al., 2016, 2015; Al-Omari et al., 2013, Ifinedo, 2012; Siponen et al., 2010; Ng et al., 2009), such as act of ignorance and forget to apply security procedures properly (Gathan Narayana Samy et al., 2010; Leach, 2003). According to Box and Pottas (2013), information security compliant behaviour is achieved through a variety of techniques. One of the techniques is increase information security awareness among users (Safa et al., 2016). This can be achieved using the technology that implemented in the organization, such as online training and security awareness campaign through website (Barlow et al., 2013; Puhakainen & Siponen, 2010).

Healthcare professionals, as the users, are a significant source of security threats, whereby their mistakes and ignorance are prone to jeopardise data (Box & Pottas, 2013; Gathan Narayana Samy et al., 2009). Therefore, this necessitates further evaluation of healthcare professionals' compliance behaviour towards ISPs related to HIS usage. To achieve this, a HIS prototype was used to further explain users' compliance behaviour towards HIS security policies. The qualitative research technique was use to collect data during prototype testing. In order to achieve RO3, the following RQ was addressed:

RQ3: How can the prototype be used to improve users' compliance behaviour towards HIS security policies?

This study assumes that the mixed-method research provides the empirical justification of the usefulness of the HISSPC model through statistical analysis (quantitative technique) and interviews (qualitative technique), which were applied during prototype testing and used to support the findings of the quantitative analysis.

1.5 Significance of the Study

This study provides a significant contribution to the underdeveloped area of research related to the HIS security behaviour and in posing numerous pertinent questions to guide future research. This study utilizes the human-technical interactions via multidisciplinary human behavioural theories to evaluate the association between the social-technical values and actions of compliance towards HIS security policies among selected Malaysian health professionals, let alone focussed on three main elements: management support, information security awareness and trust. It is important to investigate the possible factors under these elements because employees' compliance behaviour towards information security policies are likely to be influenced by many factors (Safa et al., 205; Karjalainen, 2011). In doing so, a few human behaviour theories were reviewed. Based on the reviews, there is a lack of human behaviour theories focused on the mediation effect of information security awareness and self-efficacy, particularly in respect to the relationship between management support and HIS users' compliance behaviour towards ISPs in preventing human error issues in the Malaysian healthcare sector. Moreover, very few theories adapted trust element in the area of human compliance behaviour. Therefore, this study has adapted the theoretical models imported from psychology study (HBM and TPB) and the concept of trust in information security. The HISSPC model was developed with the adaption of these theories (HBM, TPB) and trust factor. This study believes that the new model contribute to the holistic understanding of the HIS security in the Malaysian context.

Knowledge and understanding of the factors affecting the actual behaviour of health professionals towards information security may provide additional insights into health IS security incidences, as well as be of benefit to health institutions by providing solutions to improve the implementation of HIS security policies. Furthermore, they can help to promote and increase the health institution's reputation.

For academics, this study is significant as it attempts to employ more than one research method (quantitative and qualitative method). HBM and TPB are the well known human behaviour theories developed in other disciplines and these theories have been validated by IS security researchers in other areas. *Firstly*, instead of focusing solely on quantitative approach that might present a biased viewpoint of the area of interest, the qualitative approach could potentially reveal new insights into the phenomena of health professionals' compliance behaviour towards HIS security policies through prototype testing. *Secondly*, a qualitative approach would also allow the research of health professionals' compliance with IS security procedures to move beyond "Likert scale responses," by obtaining a deeper understanding of the reasons why HIS users do or do not comply with ISPs. It is believed that such an understanding can be useful for practitioners. Thus, the HISSPC model was tested efficiently and can reduce the gap in understanding of health professionals' security compliance behaviour. It is believed that the HISSPC model can be applied to other contexts of study in future.

1.6 Scope of the Study

Malaysia has government hospitals located in every state. Due to the complexity and magnitude of the programme activities, this study concentrated on government hospitals that have already implemented HIS. In Malaysia, HIS is divided into three categories: Total Hospital Information System (THIS), Intermediate Hospital Information System (IHIS) and Basic Hospital Information System (BHIS). However, this study only focused on government hospitals that implemented HIS under the THIS category because THIS, which is also known as a paperless hospital, has more complete sets of HIS, compared to IHIS and BHIS (Nurul Izzatty Ismail et al., 2013). Three government hospitals granted permission to the researcher to conduct the study – Selayang Hospital, Sungai Buloh Hospital, and Serdang Hospital.

The respondents for this study were health professionals – doctors, support staff (nurses, medical assistants, radiologists, pharmacists, and others), and health administrators –who were also the end-users of HIS and who may interact with patients or patients' data. Other than that, for development of the research framework, this study focused on the possible factors that might affect health professionals' behaviour towards ISPs by considering two main elements (management support and information security awareness).

1.7 Research Methodology

The research paradigm employed in the current study was mixed-method research in which the quantitative technique and qualitative technique were combined to collect and analyse data at some stage of the research process within a single study, to understand a research problem completely. To implement the current study, the flow of the research was divided into five phases – Initial Phase, Planning Phase, Quantitative Phase, Design and Development Phase and Qualitative Phase, as shown in Figure 1.1.

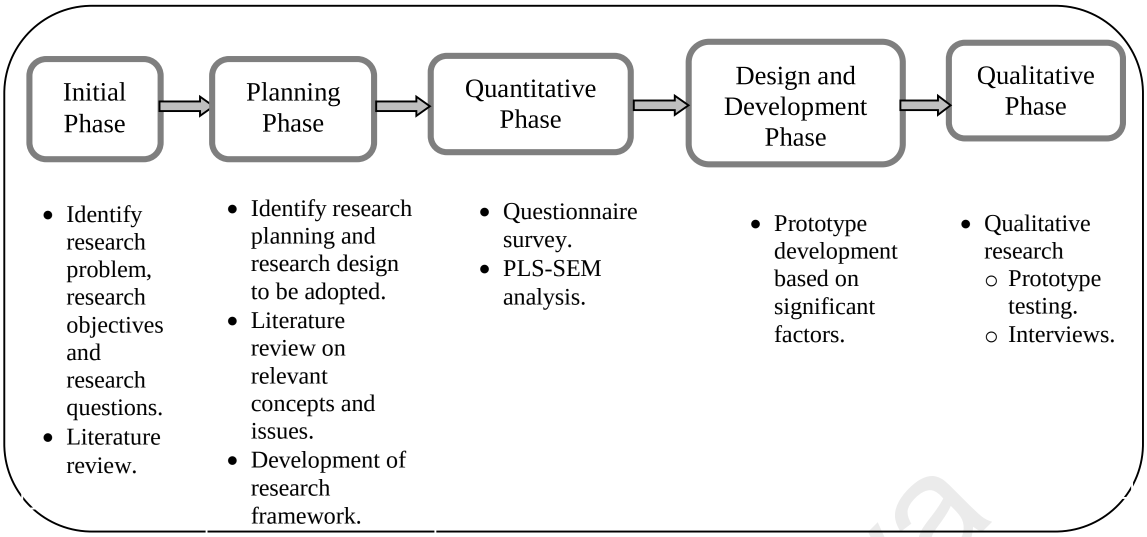

Initial Phase
Planning Phase
Quantitative Phase
Design and Development Phase
Qualitative Phase
Identify research problem, research objectives and research questions.
Literature review.
Identify research planning and research design to be adopted.
Literature review on relevant concepts and issues.
Development of research framework.
Questionnaire survey.
PLS-SEM analysis.
Prototype development based on significant factors.
Qualitative research
Prototype testing.
Interviews.

Figure 1.1: Research Methodology

In phase one, the previous literatures were reviewed to identify the research problem. Based on the research problem, the research objectives and research questions were developed.

In phase two, the factors that contribute to human compliance behaviour towards organizational security policies were explored and identified through a review of the literature. In doing so, the search strategy was important to search for the articles that were related to the current study. The researcher also needed to consider the choice of research design to accomplish the research objectives and research questions. The quantitative research technique was decided upon for the current study. Thus, the HISSPC model and research hypotheses were constructed.

In phase three, the final questionnaires were distributed to the selected local hospitals. The selected government hospitals are Selayang Hospital, Sungai Buloh Hospital, and Serdang Hospital. The questionnaires were distributed using the stratified random sampling method because the three hospitals have a different number of employees in each department. The survey data were analysed using Partial Least Squares – Structural Equation Modelling (PLS-SEM).

In phase four, the results of the survey findings led to the development of the HIS prototype. The details of the HIS prototype’s functionalities and its structures are described using Unified Modelling Languages (UML) through which the Use Case view and logical view of the prototype is modelled.

Finally, the HIS prototype was tested by HIS users with the aim of understanding the compliance behaviour among HIS users towards ISPs based on their experience using the proposed prototype. This will help to determine whether the proposed prototype is effective to improve users’ compliance behaviour towards HIS security policies in future study. The qualitative technique was used to collect and analyse the data during prototype testing. The interview data are analysed using ATLAS.ti analysis tool. This tool is a powerful workbench for the qualitative analysis of large bodies of textual, graphical, audio and video data.

1.8 Organization of Thesis

The following explains the organization of the thesis for this study:

Chapter 1

This chapter describes the background of the study, problem statement, definitions and terms used in the study. In this chapter, the research objectives and research questions of the current study are also identified and justified. The research objectives were developed based on the issue of health professionals’ compliance behaviour towards HIS security policies. The HIS security policies distributed in Malaysian government hospitals were implemented by the MOH and it is necessary for health professionals who use HIS to comply with all the security policies. Other than that, the significance of the research, research scope and a brief overview of the research methodology are also described.

Chapter 2

This chapter describes the implementation of HIS in the government hospitals in Malaysia and focuses on the functional analysis of the hospital system services, its management and the benefit of HIS to the health institutions. In addition, this chapter reviews the literature on information security and human behaviour. It examines research on HIS security, management issues, information security awareness, information security threat, human behaviour and human error. Several theories and models that are related to human behaviour and information security are reviewed and described in this chapter. The chapter ends by identifying gaps in the literature and provides the conceptual framework of the current study.

Chapter 3

The research design is described in this chapter, which covers the methodology adopted in the current study, such as the rationale for the chosen mixed-method research. It also explains how the research was conducted in terms of the search strategy, the sampling method, and the procedure for developing the survey instrument used in the current study.

Chapter 4

This chapter presents the quantitative results of the questionnaires distributed to the respondents in the three selected hospitals. The results include those from descriptive analysis, instrument items analysis, as well as the results from the Exploratory Factor Analysis and Confirmatory Factor Analysis. In this chapter, the PLS-SEM analysis findings are presented, which help the researcher identify the significant factors and lead to the development of the HIS prototype. Moreover, the discussion of PLS-SEM analysis findings also presented. This discussion covers the direct and indirect effects of the identified factors in the HISSPC model. Additionally, the findings of the moderating effect of the HIS usage experience on the relationship between the identified factors in the HISSPC model and users' compliance behaviour towards HIS security policies also discussed. Finally, the last section of this chapter discusses the linking of the quantitative and qualitative phase.

Chapter 5

In this chapter, the researcher describes the process of designing and implementing the HIS prototype. The prototype development methodology adapted in this study is the Waterfall Model, which is labelled as the Prototype Development Life Cycle (PDLC). The PDLC stages that are included in this study are the Partial Least Squares-Structural Equation Modelling (PLS-SEM) analysis, the identification of users, determining the system requirements, the interaction between objects used in the design, and finally, the prototype for implementation and testing.

In the prototype design, the use cases and the sequences of the diagrams are stated clearly. A proper use case will result in a proper sequence diagram. Furthermore, this chapter also discusses the hardware and software requirements and the design of the prototype architecture. The architectural design is modelled so that the condition and the situation of the prototype can be clearly understood. In addition, this chapter also explains and shows all the main screenshots of the module interfaces.

Chapter 6

Chapter 6 documents the experience in the implementation of the HIS prototype. It covers system testing and assessment of the users' perception concerning the HIS prototype modules that can improve users' compliance behaviour towards HIS security policies. The findings from the interview process with HIS users are also presented in this chapter. Each interview case ends with a summary of the emerging themes. The chapter end with discussion of the qualitative findings.

Chapter 7

The last chapter provides an overall discussion of the results from quantitative and qualitative analysis in line with the research questions, and implications that are vital for the future research of the development of HIS security policies for improving the strategic plans of hospitals in the field of information security system within the Malaysian healthcare sector. This chapter concludes with limitations of the study and the recommendations for future study.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter begins with the explanation of the implementation of Health Information System (HIS) in Malaysia, its aims, components, uses, and functions in section 2.2. In addition, this chapter also describes the benefits of the HIS to the health institutions. The following sections of the chapter review the literature on information security compliance behaviour and other selected constructs that are relevant to the current study. The literature review begins with a detailed explanation of information security and its threats. The next section explains the theory applied in human behaviour studies, including an illustration of the conceptual framework of this study. Reviews of the literature concerning selected constructs are also explained in the following sections. This chapter concludes with the gaps in the literature and hypotheses development of this study.

2.2 Overview of the Health Information System

Information and Communication Technology (ICT) was introduced in Malaysia in the 1990s. The rapid growth of ICT allowed the Ministry of Health to introduce HIS in several local hospitals. The HIS implemented in hospitals integrates several sub-systems, which are designed to manage the administrative, financial, and clinical aspects of hospitals to provide the best services to patients and manage hospital records effectively. HIS plays a major role in planning, initiating, organizing, and controlling the operations of the subsystems of the hospitals, and thus, provides a synergistic organization in the process (Aniza Ismail et al., 2010).

In Malaysia, HIS integrates two or more information systems that are differentiated by their core functions, the departments that use them and the types of user. The major information systems that are implemented in public hospitals are Clinical Information System (CIS), Financial Information System (FIS), Laboratory Information System (LIS), Nursing Information System (NIS), Pharmacy Information System (PIS), Picture Archiving Communication System (PACS), and Radio Information System (RIS), as shown in Figure 2.1 as cited by Nurul Izzatty Ismail & Nor Hazana Abdullah (2012).

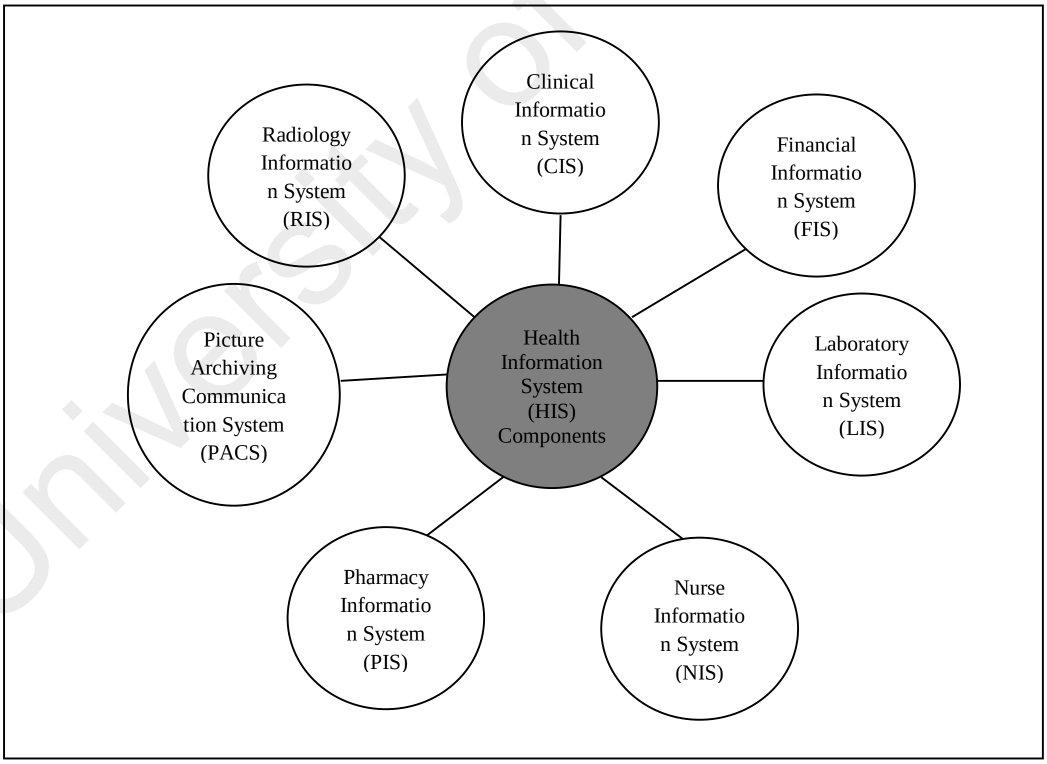

Clinical Informatio n System (CIS)
Radiology Informatio n System (RIS)
Financial Informatio n System (FIS)
Picture Archiving Communica tion System (PACS)
Health Information System (HIS) Components
Laboratory Informatio n System (LIS)
Pharmacy Informatio n System (PIS)
Nurse Informatio n System (NIS)

Figure 2.1: HIS Components (adapted by Biomedical Informatics Ltd., 2006, as cited by Nurul Izzatty Ismail & Nor Hazana Abdullah (2012))

Another information system (IS) used in some public hospitals is the Patient Management System. Although the HIS components are many, as shown in Figure 2.1, not all of these components in HIS are used in public hospitals in Malaysia, and different hospitals might use different combinations of HIS components. The HIS component that is used most in the public hospitals is the CIS (Nurul Izzatty Ismail & Nor Hazana Abdullah, 2012). Table 2.1 shows the differences between each component by their function, department and type of user.

Table 2.1: Differences between HIS Components (As cited by Nurul Izzaty and Nor Hazana Abdullah, 2012)

HIS component	**Differences**		
	Function	**Department**	**Type of User**
CIS	Designed to collect, store, manipulate, process, and deliver healthcare information.	Clinical	Doctors, Nurses
FIS	Manages business aspects of hospital, such as processes financial information.	Financial	Accountant
LIS	Manages laboratory information, such as clinical chemistry, haematology and microbiology.	Laboratory	Lab Officers
NIS	Manages clinical data from a variety of healthcare environments with the aim to improve patient care.	Ward	Nurses, Doctors
PIS	Manages pharmacy information.	Pharmacy	Pharmacists
PACS	Facilitates the archiving, processing, and viewing of digital radiological images and related information.	X-ray Imaging	Imaging Officers
RIS	Assists radiology services in storing, manipulating, and retrieving information.	Imaging	Imaging Officers

Basically, each HIS component caters to a specific need or function, and is used by different types of user. For example, CIS and NIS are used by doctors and nurses. CIS was developed to collect, store, manipulate, process, and deliver health information in the Clinical Department or any department that requests the records. Meanwhile, NIS was developed to manage clinical data from a variety of healthcare environments, and usually this system is operated in the wards of the hospital. PACS and RIS are used by Imaging Officers and assist the digital and radiology services in terms of storing and retrieving X-ray and image information. All the laboratory information is managed by Lab Officers using LIS, and hospital financial information is managed by hospital accountants through FIS.

2.2.1 Categories of HIS

HIS is divided into three categories – Total Hospital Information System (THIS), Intermediate Hospital Information System (IHIS), and Basic Hospital Information System (BHIS). Hospital size is vital to indicate the HIS categories, in as much as THIS is for hospitals with more than 400 beds, IHIS is for hospitals with 200 to 400 beds, and BHIS is for hospitals with less than 200 beds (Nurul Izzatty Ismail et al., 2013; Lee, Ramayah, & Zakaria, 2012). Moreover, the different sets of IS implemented in the hospitals also represent the category of HIS, as shown in Table 2.2. THIS, which is also known as a paperless hospital, has more complete sets of HIS than IHIS and BHIS.

Table 2.2: Public Hospitals Implementing HIS (As cited by Nurul Izzatty Ismail et al., 2013)

Categories of HIS	Hospitals	Components of HIS	Number of Beds
1) THIS	Selayang Hospital, Putrajaya Hospital, Serdang Hospital, Sungai Buloh Hospital, Pandan Hospital, Ampang Hospital, Alor Setar Hospital, Sungai Petani Hospital, Sultanah Zahirah Hospital, Sultan Haji Ahmad Shah Hospital, and Bintulu Hospital.	Patient Management System + CIS + LIS + PIS + RIS + PACS + Administration Information System + FIS + Inventory Information System + Personnel Information System	More than 400 beds
2) IHIS	Keningau Hospital, Lahad Datu Hospital	Patient Management System + CIS + LIS + PIS	More than 200 beds, but not less than 400 beds
3) BHIS	Kuala Batas Hospital, Setiu Hospital, Pekan Hospital, Pitas Hospital, Kuala Penyu Hospital, Kunak Hospital, Tuanku Ja'afar Hospital, and Port Dickson Hospital	Patient Management System + CIS	Less than 200 beds

Selayang Hospital was the first paperless hospital to operate on THIS in the year 1990 (Lee et al., 2012; Aniza Ismail et al., 2010), which integrates clinical, administrative, and financial management, enabling a seamless data flow between separate areas, as shown in Figure 2.2. Then, THIS was implemented in other hospitals, such as Putrajaya Hospital and University Kebangsaan Malaysia Medical centre (UKMMC).

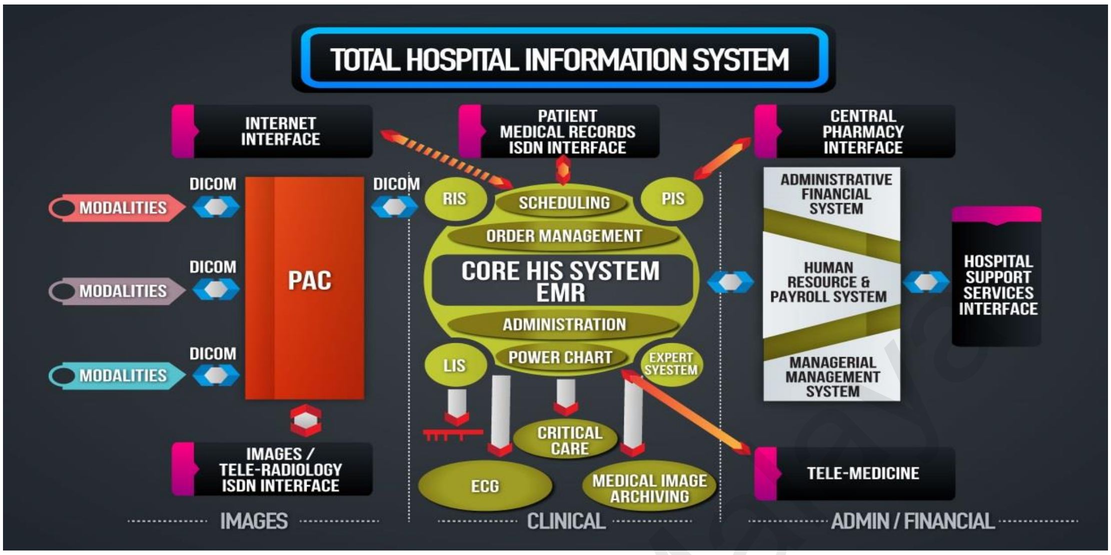

TOTAL HOSPITAL INFORMATION SYSTEM
INTERNET INTERFACE
PATIENT MEDICAL RECORDS ISDN INTERFACE
CENTRAL PHARMACY INTERFACE
DICOM
MODALITIES
DICOM
MODALITIES
DICOM
MODALITIES
PAC
DICOM
RIS
SCHEDULING
PIS
ORDER MANAGEMENT
CORE HIS SYSTEM EMR
ADMINISTRATION
LIS
POWER CHART
EXPERT SYESTEM
CRITICAL CARE
ECG
MEDICAL IMAGE ARCHIVING
ADMINISTRATIVE FINANCIAL SYSTEM
HUMAN RESOURCE & PAYROLL SYSTEM
MANAGERIAL MANAGEMENT SYSTEM
HOSPITAL SUPPORT SERVICES INTERFACE
IMAGES / TELE-RADIOLOGY ISDN INTERFACE
TELE-MEDICINE
IMAGES
CLINICAL
ADMIN / FINANCIAL

Figure 2.2: Total Health Information System (Sources from Selayang Hospital)

THIS in Selayang Hospital has divided HIS components into three categories of information system – image management (PACS), clinical information (RIS, PIS, LIS and CIS), and administration and financial information. Administration and financial IS have several subsystems – administrative and financial information system, human resources and payroll system, and material management IS.

2.2.2 Uses and Functions of HIS

HIS provides information for the management of health programmes and services. In particular, it is essential for monitoring the health situation, the performance of promotive and curative health services and activities, and the availability and utilization of health resources. HIS is made up of mechanisms and procedures for acquiring and analysing data, and for providing the information needed by (Nurul Izzatty Ismail & Nor Hazana Abdullah, 2012; Chang, 2011; Barakat, 2002):

(i) All levels of health planners and managers for the planning, programming, budgeting, monitoring, assessment, and coordinating of health programmes and services.

(ii) Health care personnel, health researchers, and educators in support of their respective activities.

(iii) Socio-economic planners and the general public outside the health sector for inter-sectorial information linkage.

(iv) National policymakers for formulation of evidence-based policy.

The functions of HIS are described as follows (Nurul Izzatty Ismail & Nor Hazana Abdullah, 2012):

(i) To measure the health status of the communities and to quantify their health problems, and medical and health care needs.

(ii) For local, national, and international comparisons of health status. For such comparisons, the data need to be subjected to rigorous standardization and quality control.

(iii) For planning, administration and management of health services and programmes.

(iv) For accessing other health services and accomplishing their stated objectives in terms of effectiveness and efficiency (quality assurance).

(v) For assessing the attitudes and the degree of satisfaction of the beneficiaries towards the health system at various points of time.

(vi) For training and education of the current and future health workers.

2.2.3 Benefits of HIS

HIS implementation in the healthcare sector is significant to our country because the system can improve healthcare quality services in most Malaysian public hospitals. Moreover, HIS has various advantages to improve the hospital filing system, as follows (Lee et al., 2012; Nurul Izzatty Ismail & Nor Hazana Abdullah, 2012; Hidayah Sulaiman, 2011):

(i) Cost reduction by coordinating services.
By integrating information systems in HIS, it can reduce the cost to manage hospital data.

(ii) Excellent and modern infrastructure that can increase the speed of the health care service and accuracy to improve quality of care. HIS can help to reduce transcription errors and duplication of data entries. In addition, hospital data are more accessible and easier to search.

(iii) Hospital tasks can be managed more systematically.

(iv) The communication between healthcare providers is improved.

2.3 Information Security

Information security issues are the major issues in e-commerce studies, such as online banking and online shopping. Today, this has progressed to health institutions because the institutions have embarked on HIS, which can be accessed through a network (Alemdar & Ersoy, 2010). Health information is very sensitive and confidential, thus the data require security protection because if a patient's data are exposed to an unauthorized user, it might jeopardize the patient. Health data contain the details of a person's family history, genetic testing, history of diseases and treatments, history of drug use, sexual orientation, practices and testing for sexually transmitted disease, patient's demeanour, character, and mental state (Tesema et al., 2010). Improper disclosure or misuse of data can cause serious harm to the patient, such as discrimination, stigmatization, or loss of insurance or employment (Liginlal et al., 2012). Therefore, information security plays an important role in protecting health data from theft and abuse. Information security in health institutions is used to protect health data from unauthorized access, use, disclosure, disruption, modification or destruction (Box & Pottas, 2013; Tesema et al., 2010).

The literature also defines information security as the protection of information systems from unauthorized access and information threats, focusing on three elements: confidentiality, integrity, and availability (Cavalli et al., 2004). Health records require strong confidentiality as health information is important for patient's medical (Hass, Wonlgemuth, Echizn, Somehara, & Muller, 2010). Meanwhile, integrity is essential for correct treatment. Moreover, availability is also as important as integrity because health information in HIS might be necessary for adequate treatment, and thus, health information should be available as needed by health professionals.

2.4 Threats to Information Security

A threat is defined as any unexpected or potential cause of an unwanted incident that impacts negatively on a system or organization (Symantec, 2013; Gathan Narayana Samy et al., 2010). Information security threats are serious and should be controlled and monitored by organizations because they have the potential to cause harm (Alhabeeb et al., 2010). Information security threats can be divided into two types: external and internal threats. An external threat is caused by an outsider, which is easily controlled using security technology such as firewalls (Safa et al., 2016; Colwill, 2009). However, internal threats are caused by insiders or employees of the organization that are difficult to manage (Purpura, 2013; Williams, 2008) because they have legitimate and often privileged access to facilities and organizational information, have knowledge of the organization and its processes, and know the location of critical or valuable assets (Colwill, 2009).

Internal threats can be malicious (employees who plan to take revenge and financial gains) or non-malicious (human error) (Sarkar, 2010). Many organizations are unaware that internal threats can cause harm, such as stealing, and destroying an organization's information can cause unwanted security incidents. Moreover, according to Sarkar (2010), attacks by insiders are difficult to detect compared to the foot printing activities of an external hacker. Thus, an organization is required to invest more in human capital rather than technology alone in combating information security threats (Da Veiga & Martins, 2015). The people who are attached to the organization implement the technology, and thus, without proper education and knowledge concerning information security, would not be able to practice it appropriately (Safa et al., 2015; Shropshire et al., 2015).

The classification of information security threats is extensive in the IS security literature. Guo (2012) divided information security threats into four dimensions; (i) sources, which could be internal or external to the organization in question; (ii) perpetrators, which could be either human or non-human; (iii) intent, which could be intentional or unintentional (accidental); and (iv) consequences, which could be disclosure, modification, destruction, or denial of service. Threats can also be accidental or deliberate (Jung, Han, & Lee, 2001). Accidental threats can be natural disaster and human errors or omissions, whereas deliberate threats are intentional acts, such as computer fraud, embezzlement, and theft. Other literature categories of threats to IS are three types, as follows (Gathan Narayana Samy et al., 2010):

(i) Natural (similar to other studies that identify natural disasters, such as floods, earthquakes, tornadoes, landslides, and electrical storms)

(ii) Human (unethical or deliberate acts)

(iii) Environmental (pollution, chemical spills, and liquid leakage)

Gathan Narayana Samy et al. (2010) also revealed that the five most critical categories of threats to HIS are power failure (e.g. server down and service provider interruption), human error (e.g. entry of erroneous data by employees and accidental deletion or modification of data by employees), technological obsolescence (e.g. outdated hardware and software installations), hardware failure (e.g. hardware maintenance error), and software failure (e.g. software maintenance error).

The issues related to technology can be easily managed by the organization. However, human error issue can be complex and challenging (Safa et al., 2015; Ifinedo, 2014; Al-Omari et al., 2013; Sarkar, 2010; Liginlal et al., 2009). In the medical environment, technology and networks have been used to facilitate patients' care and services (Nurul Izzatty Ismail et al., 2013). Medical records can be transferred online. However, this can result in the potential impact of human error if not monitored carefully. Information security threats may not prevent medical practice from functioning in its ability to provide patient care, but it can cause inconvenience and affect the efficiency with which it is delivered (Brady, 2011; Williams, 2008). Security incidences are costly as patients and health information are key assets in medical practice. Brady (2011) and Williams (2008) also argued that security incidences, such as loss of data, loss of integrity and availability or breaches of confidentiality, can result in efficacy and legal problems. Therefore, health institutions must seriously consider the issue of information security threat and identify security strategies to increase information security awareness among their employees.

2.5 Human Error

One of the failures to IS security is due to unacceptable user behaviour (Akhunzada et al., 2015; Tetlock, Vieider, Patil, & Grant, 2013; Brady, 2011; Moller, Ben-Asher, Engelbrecht & Englert, 2011). No matter how good the system security being implemented in the organization, ultimately, the security posture depends on appropriate user behaviour (Rhee et al., 2009). Unacceptable user behaviour is often referred to as human error in other studies (Al-Omari et al., 2012a; Abdul Rahman Ahlan et al., 2011; Gathan Narayana Samy et al., 2010; Liginlal et al., 2009). Human error can be defined as "*a change in human performance which causes a deviation from a desired success path, which then leads to an undesired or unplanned result"* (Wood & Banks Jr, 1993, p. 52). Many studies have agreed that human error is a major issue in computer security (Akhunzada et al., 2015; Colwill, 2009; Gathan Narayana Samy et al., 2010; Wood & Banks Jr, 1993). Human error can be a major risk to an organization if the organization does not have the capability to control and manage it accordingly through the implementation of Information Security Policies (ISPs) (Abdul Rahman Ahlan et al., 2011). ISPs provide security guidelines and procedures that employees must follow (Al-Omari et al., 2012b) and human error arose from poor ISPs formulation and implementation (Liginlal et al., 2009). Moreover, Parsons et al. (2014) stated that management of the organizations were most concerned about human error, as they felt that security breach were more likely to be caused by security unawareness and naivety behaviour.

Human error is caused by employees, either deliberately or accidentally. Deliberate cause exists when employees have a grudge against their employer because they feel angry and dissatisfied with their employer (Kreicberga, 2010; Leach, 2003). Many human errors reported in the studies are caused by accidental acts because of user slips and mistakes due to a lack of information concerning security skills and lack of knowledge towards information security (Liginlal et al., 2009; Renaud, 2012; Vroom & von Solms, 2004). According to Liginlal et al.(2009), human slips occur as an outcome of the incorrect execution of a correct action sequence, which usually happens because of human carelessness, such as inadequate written communication (prescriptions, documentation, transcription) (Keers et al., 2013). Meanwhile, human mistakes occur as an outcome of the correct execution of an incorrect action sequence, i.e., wrong decisions executed correctly because of human ignorance, and failure to comply with an organization's rules and procedures (Boujettif & Yongge, 2010; Gathan Narayana Samy et al., 2009). For an example, the behaviour like sharing password with other people. This is supported by other studies in which human error occurs when a person fails to take the correct action that is required, especially when implementing ISPs (Wood & Banks Jr, 1993). For example, one who forgets to back up a hard disk or does not create a strong password. Liginlal et al. (2012) compiled a list of eight possible causes of human error that lead to security breaches as shown in Table 2.3.

Table 2.3: Perceived causes of human error (compiled from Liginlal et al, 2012)

Perceived Causes of Human Error	**Illustrative Example**
Lack of knowledge of organization's security rule	Shredding of confidential documents or emailing the document to wrong addressee
Poor discipline of employees	Laziness, arrogance, indifference
Poor skills of employees	Computing skills, communication skills, work related skills
Inefficient business process and inefficient workflow	Redundancy, bottlenecks, sub-optimality

Perceived Causes of Human Error	Illustrative Example
Physical environment limitations	Small room where everyone can overhear
Technology limitations	Outdated computer applications, computer sharing, slow network
Organizational limitations	Understaffed, high turnover, low morale, high workload
Poor monitoring and poor enforcement	Few incentives to comply or penalties for violations

The issue of human error must be seriously considered by organizations because although employees' roles are vital to the success of the organization, they are the weakest link when it comes to information security. Thus, organizations must inject adequate information security behaviour to everyone who works in the organization, who are also the end-users. Information security behaviour is described as a set of core information security activities that has to be adhered to by end-users to maintain information security as defined by the organization's ISPs (Renaud, 2012).

Koskosas, Kakulidis & Siomos (2011) stated that employees must be proactive in information security. If all the organizational practices recommended information security behaviour, the level of user awareness can be increased. It is also believed that the information security behaviour might have an effect on the success or failure of the information security process in the organization, especially in the medical domain. Thus, the management needs to control and monitor their employee behaviour concerning information security because health information is sensitive and requires high confidentiality (Lechler, Wetzel, & Jankowski, 2011).

2.6 Information Security Compliance Behaviour

IS security can be implemented more effectively if users' behaviour towards information security can be controlled and managed accordingly. Or else, it can pose threats to the organization's information security. IS security effectiveness is defined as the ability of IS security measures to protect against the unauthorized and deliberate misuse of assets of the (Liginlal et al., 2012) local organizational IS by individuals, including violations against hardware, software, data, and computer services (Brady, 2010; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005). Kankanhalli et al. (2003) argued that deterrents and preventive efforts by the management can contribute to the effectiveness of information system security in the organization. Meanwhile, Woodhouse (2007) suggested that the effectiveness of IS security can be achieved through promoting adequate information security behaviour and constraining unacceptable information behaviour among employees in the organization. The current study believes that if user compliance behaviour towards information security is acceptable, security incidences can be decreased, and the effectiveness of IS security can be increased. This is also supported by other information security studies, where security compliance behaviour can promote security assurance behaviour, such as employees will be more careful in handling an organization’s data (Rocha Flores, Antonsen, & Ekstedt, 2014; Guo, 2012; Warkentin et al., 2011).

Previous studies describe information security compliance behaviour as behaviour that does not violate an organization’s ISPs (Guo, 2012) and adheres to a set of core information security activities as recommended by the organization (Padayachee, 2012). Most of the ISPs are developed from the security requirements in an organization to suit their own objectives (Parsons et al., 2014; Noor Hafizah Hassan & Zuraini Ismail, 2012). Organization’s ISPs usually consists of several focus areas such as password management, information handling, among others as shown in Table 2.4.

Table 2.4: Examples of ISPs focus and sub-areas (As cited by Parsons et al, 2014)

Focus area	Sub-areas
Password management	Locking workstations Password sharing Choosing a good password
Email use	Forwarding emails Opening attachments IT department level of responsibility
Internet use	Installing unauthorised software Accessing dubious websites Inappropriate use of Internet
Social networking site (SNS) use	Amount of work time spent on SNS Consequences of SNS
Incident reporting	Reporting suspicious individuals Reporting bad security behaviour by colleagues Reporting all security incidents
Mobile computing	Sending sensitive information via mobile networks Checking work email via free network
Information handling	Disposing of sensitive documents Inserting DVDs/USB devices Leaving sensitive material unsecured

The goals of information security are to maintain security compliance among users and to achieve competitive edge (ISO/IEC 17799:2000 Information Technology, as cited by Saint-Germain, 2005). For example, in term of password management, employees are required to always logging off their computer when the computer is unattended and not sharing their password and user name with other colleagues (Launders & Polovina, 2013). Meanwhile, in terms of email and Internet use, it is considered as inappropriate security behaviour if employees opening unsolicited email attachment and accessing dubious websites. Moreover, in the ISPs also stated that employees are not allowed to access Social Network System (SNS) during work time and leave documents that contain sensitive information on a work desk overnight (Launders & Polovina, 2013).

Employees are also responsible to report all security incidents to the management and sending work emails using only secure networks as this is also considered as ISPs compliance behaviour. ISPs compliance behaviour among employees can be improved if the organization provides a clear policies instruction to all employees (Da Veiga & Martins, 2015). For example, a security policy might state, *"Employees must log off their computers when not at their work desks"*. According to Boss, Kirsch, Angermeier, Shingler and Boss (2009), this policy addresses two possible concerns: the issue of accountability in that someone might use the available computer (many systems are set to require a password to unlock after 10-15 min of activity) and thus not be held accountable for their actions; and to limit the amount of time a hacker has to attack a specific active user. Likewise, another clear policy could be *"Reporting any security incidents existed in the organization"*, whereby this policy requires users to recognise security threats.

Information security compliance behaviour is dependent on combinations of several factors that fall under organizational, technology, and also personal factors (Safa et al., 2015; Brady, 2010; Chan, Woon & Kankanhalli, 2005). It is very important to understand the factors that influence user's behaviour because it could provide helpful benefits for information security professionals with an interest in assessing the effectiveness of an information security programme (Rhee et al., 2009; Stanton, Stam, Mastrangelo & Jolton, 2005). An effective information security programme could increase user awareness towards information security and promote good user information security behaviours (Ng et al., 2009). If users are not motivated to follow organization's rules and procedures to protect information, security might fail; hence, management play an important role to ensure the effectiveness of information security programme (Waly, Tassabehji & Kamala, 2012).

There are several reasons why users do not comply with security rules and procedures, which include the feeling that the security rules and policies are too strict, have lower usability, are a nuisance, complicated, and difficult to follow (Renaud, 2012). In addition, the non-compliance behaviour towards security policies is also due to user dissatisfaction and lower usability of the system security that has been developed by the system developer (Herath & Rao, 2009a). There are various factors that lead to non-compliance behaviour events, and even though management provides effective information security training, employees still make mistakes. These factors are divided into three dimensions: environmental, social, and organizational factors (Brady, 2011; Hovav & D'Arcy, 2012). If their work environment is stressful, it might reduce their attention and cause errors (Parsons et al, 2014). Social and organizational factors may influence them to comply and behave properly towards information security (Hovav & D'Arcy, 2012). If the peers and superiors of the employees do not bother or care to follow the security rules and procedures, neither will they, therefore, it is very important that everyone in the organization practices a positive security environment at their workplace because it can help to increase IS security effectiveness, and hence, security incidences can be decreased.

Moreover, many security breaches are contributed by human error due to poor security behaviour by employees (Kreicberge, 2010; Leach, 2003), such as negligence and ignorance (Da Veiga & Martins, 2015; Safa et al., 2015). Hence, it is very important for an organization to focus on strategies to improve user security behaviour by identifying and understanding the factors that might influence user behaviour. The factors are divided into two groups, as shown in Figure 2.3, whereby the first group describes a user's understanding of what behaviours are expected by others, and the second group describes a user's willingness to constrain their behaviour to stay within accepted norms (Leach, 2003).

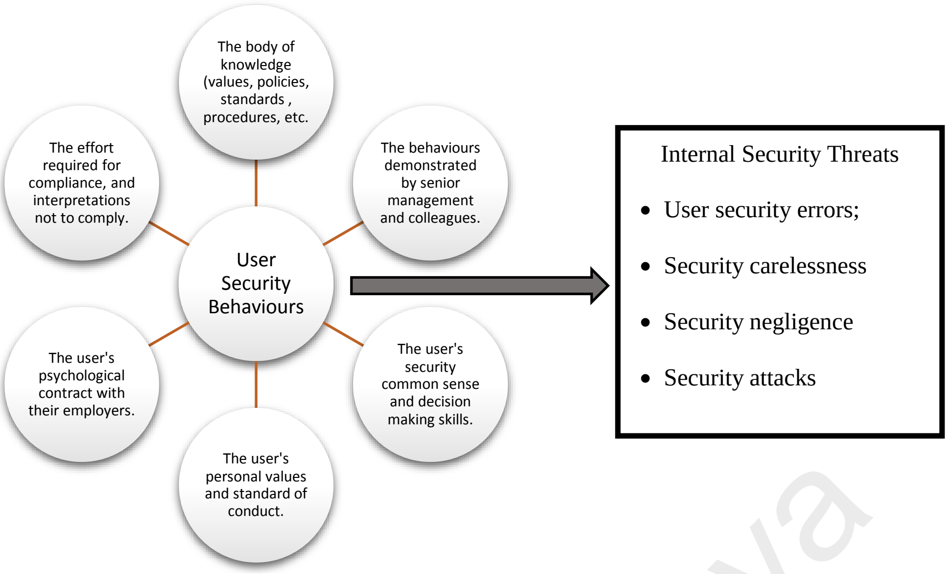

The body of knowledge (values, policies, standards , procedures, etc.
The effort required for compliance, and interpretations not to comply.
The behaviours demonstrated by senior management and colleagues.
User Security Behaviours
The user's psychological contract with their employers.
The user's security common sense and decision making skills.
The user's personal values and standard of conduct.
Internal Security Threats
User security errors;
Security carelessness
Security negligence
Security attacks

Figure 2.3: The factors that influence user's security behaviour (As cited by Leach, 2003)

The users' understandings of which behaviours are expected of them are formed from the following (Da Veiga and Martins, 2015; Shropshire et al., 2015; Leach, 2003):

(i) What they have been told, which can be done through the implementation of ISPs and procedures that the organization documents for their employees to read and comply with.

(ii) What they see when others practice the behaviour, whereby their behaviour can be influenced by their colleagues and superiors. Thus, it is important for the organization to create a good culture among their employees. The top management needs to control and monitor their employees to ensure that they comply with the ISPs and procedures by injecting good messages and motivate them in proper ways. According to Da Veiga and Martins (2015), information security awareness and training programmes are the factors that can influene information security culture among employees.

(iii) Their experience built from decisions they have made in the past, as this is influenced by their past experience when they feel that it is beneficial to comply with all the policies and procedures.

In addition, the human factors that influence user behaviour or willingness to constrain their behaviour to stay within those norms are affected by the following:

(i) Their personal values and standards of conduct, in that most employees ascribe high value to principles and believe in the importance of shared values and sensible rules (Safa et al., 2016; Bulgurcu et al. 2009; Leach, 2003). Therefore, they will easily follow and comply with any organizational rules and procedures.

(ii) Their sense of obligation towards their employer, which can be influenced by how the employer treats employees in the organization, either pressures them or recognizes and rewards them (Brady, 2010; Herath, 2008). If the employees feel that they are well treated, they will respond in kind and act in the organization's best interest, otherwise they would feel angry.

(iii) The degree of difficulty that employees experience in complying with the company's procedures (Warkentin et al., 2011), whereby, if employees feel that security control is difficult to perform and complicated, they might not comply. Thus, it is very important for the organization to plan a security strategy to ensure that it can be delivered to the employees effectively and that the right message is conveyed.

2.7 Theoretical Review

Several theories were reviewed in order to find the most appropriate theory to be adapted and then further developed into a new research model. The previous literature revealed some theories that investigated user behaviour towards IS technology, such as the Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), and Theory of Planned Behaviour (TPB), among others.

Leach (2003) described that human behaviour can be influenced by two groups of factors, as explained in the previous section. The first group describes what user understands of what behaviours are expected by other employees, and the second group describes users' willingness to constrain their behaviour to stay within accepted norms based on their beliefs. This is similar to the ***Social Cognitive Theory (SCT),*** in which personal and environmental factors are known to affect human behaviour bidirectionally (Bandura, 1989). This is illustrated in Figure 2.4.

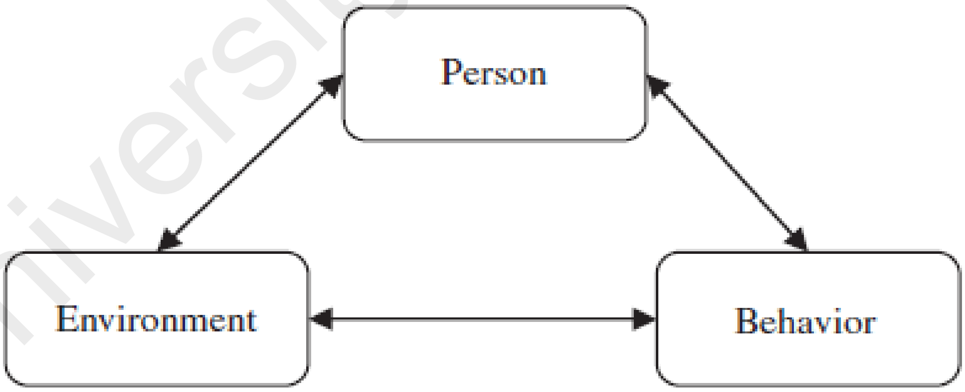


Figure 2.4: SCT Model (Bandura, 1989)

Furthermore, SCT describes that human expectations, beliefs, emotional benefits and cognitive competencies are developed and modified by social influences that convey information, and activate emotional reactions through modelling, instruction, and social persuasion (Bandura, 1989; Siwei & Xiaoping, 2009). Personal factors, such as age, race, sex, and others can also influence humans to evoke different reactions from their social environment (Rhee et al., 2009). Chiu, Hsu and Wang (2006) describe SCT as a theory that defines human behaviour as a triadic, dynamic and reciprocal interaction of personal factors, behaviours, and social network. The literature suggested that self-efficacy and outcome expectations are the factors that affect human behaviour. This is argued by Bandura (1989) who explained that a person’s behaviour is developed and controlled by the influences of their social network and the person’s cognition (e.g. expectations and beliefs).

SCT is a widely accepted theory that has been adapted in several different areas of studies for validating human behaviour, such as cancer (Basen-Engquist et al., 2011), IS team development knowledge contribution (Chang, Yen, Chiang, & Parolia, 2013), and programmer perception on knowledge sharing (Tsai & Cheng, 2010). These studies have found that social cognition strongly affects humans to perform certain behaviours, such as cancer preventive behaviour, knowledge contribution and sharing. In information security studies, social cognition was also found to influence security compliance behaviour (Johnston & Warkentin, 2008; Myyry et al., 2009). This is also argued by authors in recent studies, whereby social cognition play an important role in influencing information system security policies compliance behavior (Tsohou et al., 2015; Ifinedo, 2014).

Health Belief Model (HBM) was formulated by Rosenstock (1974) and it was widely used in health behaviour studies, such as drug (Bonar & Rosenberg, 2011), cancer (Bylund, Galvin, Dunet, & Reyes, 2011) and dental (Buglar, White, & Robinson, 2010). HBM predicts that if people believe in specific illnesses and know how to prevent the illnesses, they will be more cautious, and therefore practice recommended healthy behaviour (Gammage & Klentrou, 2011). HBM suggests that individuals determine the feasibility, benefits, and cost related issues to an intervention or behaviour change based on the following factors: perceived susceptibility (similar to perceived vulnerability), perceived benefits, perceived barriers, cues to action, and perceived seriousness (severity), as shown in Figure 2.5.

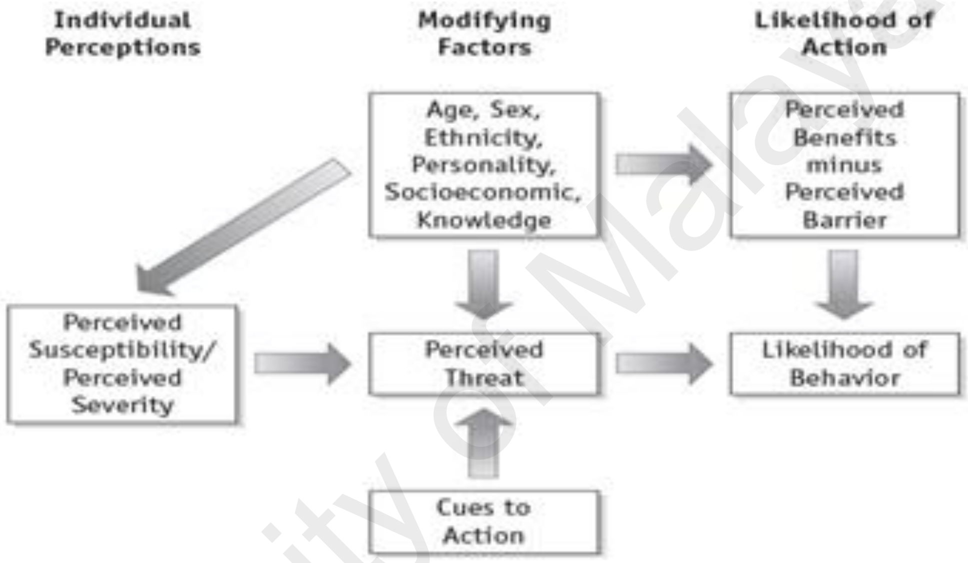

Individual Perceptions
Modifying Factors
Likelihood of Action
Age, Sex, Ethnicity, Personality, Socioeconomic, Knowledge
Perceived Benefits minus Perceived Barrier
Perceived Susceptibility/ Perceived Severity
Perceived Threat
Likelihood of Behavior
Cues to Action

Figure 2.5: Health Belief Model (Rosenstock ,1974)

Susceptibility refers to the subjective risks of contracting a condition (Rosenstock, 1974). Other author also defines perceived susceptibility as a person’s evaluation of his or her probability of being exposed to malicious threats (Woon, Tan & Low, 2005). In health studies, perceived susceptibility is one of the powerful perceptions that affect people to adopt healthier behaviours. If people feel that they have low susceptibility, this may result in unhealthy behaviour (Şimşekoğlu & Lajunen, 2008). This is similar in the information security context as well, whereby if high susceptibility is perceived by people, they will be motivated to adopt information security behaviours (Younghwa, 2011). Perceived susceptibility has also been shown as a determinant in computer security behaviour (Claar & Johnson, 2012; Vance et al., 2012; Ng et al., 2009), and to evaluate a person’s probability of being exposed to malicious threats (Woon & Kankanhalli, 2007).

Meanwhile, perceived severity refers to an individual’s belief in the seriousness of certain circumstances (Bylund et al., 2011). In health studies, if people perceive the seriousness of disease or any deviant behaviour, they will adopt healthier behaviours and practice them adequately (Ross, Ross, Rahman & Cataldo, 2010). According to Rosenstock (1974), the degree of seriousness of a given health problem may be judged both by the degree of emotional arousal created by the thought of a disease as well as by the kinds of difficulties the individual believes a given health condition will create for him. Similarly, in information security studies, perceived severity has been found to prevent employees’ violation behaviour towards ISPs (Cheng et al., 2013). Perceived severity also reported to influence employees’ behaviour towards complying with an organization’s ISPs (Chenoweth et al., 2009). Huang et al. (2011) suggested that users’ security compliance behaviour can be enhanced by changing their perception towards threat severity. Meanwhile, Herath and Rao (2009b) found that the severity of punishment has a negative effect on users’ intention in terms of security behaviour.

Perceived benefit in health research refers “*to what the person perceives as the positive outcome of performing certain health behaviours*” (Bylund et al., 2011). People tend to adopt healthier behaviour if they believe that the recommended behaviour can improve their health (Rosenstock, 1974). Rosenstock also argued that an individual’s beliefs about the effectiveness of various courses of action determine what course that he or she will take. This is similar to the context of information security whereby if users perceive the benefits of complying with an organization’s ISPs such as using security-countermeasures, they will practice information security behaviour adequately. Previous studies have found that the perceived benefit determines information security behaviour (Bulgurcu et al., 2009; Ng et al., 2009) and significantly influence computer security usage of IS users (Clarr, 2011). This is also supported by recent research finding, whereby many users are rarely touched on the possible benefits of adopting secure behaviour such as confidence in using security software and ISPs (Davinson & Sillence, 2014).

An individual may be believed that certain preventive behaviour will be effective to reduce the threat of disease. However, the preventive behaviour may be inconvenience, unpleasant, paintful and upsetting that serve as barriers to action and this will cause avoidance (Rosenstock, 1974). In health research, a perceived barrier is defined as a person's evaluation "of the potential obstacles that may lessen the likelihood of engaging in healthy behaviour" (Welsh et al., 2011). Several barriers that reduce people to engage in healthy eating behaviour, were identified such as lack of knowledge, lack of self-control, and lack of time (Hanson & Benedict, 2002). Similarly, in IS studies, if users feel that adopting information security behaviour is difficult and slows down their daily work, it will cause non-compliance behaviour of ISPs among employees in the organization (Ng et al., 2009). Claar and Johnson (2012) found that perceived barriers negatively influenced security behaviour among website users. This is because, if users perceive a security threat sufficiently, they will be more cautious and any barriers related to adopting security behaviour can be reduced.

In addition, the authors of previous studies have argued that human behaviour can be controlled based on their perceptions of security threats and how this can help them to perform adequate behaviour to reduce threats (Hovav & D'Arcy, 2012; Ng et al., 2009). The perception of a security threat is likely to be affected by the susceptibility and severity, and evaluation of the secure behaviour is likely to be affected by the benefits and barriers; hence, if a threat is perceived and secure behaviour is chosen, the users know how to behave and conduct themselves properly (Davinson & Sillence, 2010).

On the other hand the ***Protection Motivation Theory (PMT),*** which is a theory that is adapted from HBM, was introduced by Roger in 1975. This theory *“explains how people change their health attitude and behaviours in response to health risk message”* (Moller et al., p. page 4). For example, if a threat is perceived by people as fearful, they would prevent the possible threat. On the other hand if an individual has good knowledge concerning security threats and perceives the effectiveness of security policies as a coping mechanism, they will believe that complying with the organization’s security policies is important (Herath & Rao, 2009b).

PMT is based on five factors that are believed to motivate users to protect themselves, namely, severity, vulnerability, response cost, and response efficacy, as shown in Figure 2.6. These factors are divided into two categories: threat appraisal (Severity and Vulnerability), and coping appraisal (Response Cost and Response Efficacy). Threat appraisal states that if people have a strong perception concerning the severity and vulnerability of a threat, it can motivate them to avoid security incidences (Younghwa, 2011; Prentice-Dunn & Rogers, 1986). Meanwhile, coping appraisal refers to the ability of people to avoid security risk and believe that they can practice the recommended security behaviour successfully (Plotnikoff, Trinh, Courneya, Karunamuni, & Sigal, 2009; Prentice-Dunn & Rogers, 1986).

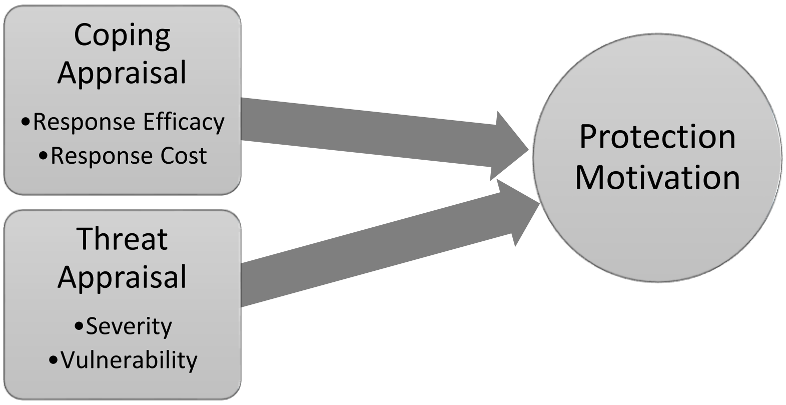


Figure 2.6: Protection Motivation Theory (Prentice-Dunn & Rogers, 1986)

PMT was applied successfully in over 30 different domains, such as cancer (Cox, Koster, & Russell, 2004), anti-drug abuse (Fry & Dann, 2002), and online harassment behaviour (Lwin, Li, & Ang, 2011). Most of these studies showed the positive effects of PMT factors on the subject. For example, if a threat is highly perceived by people, it can prevent deviant behaviour either in health or in information security. Additionally, recent information security studies also found that most of the PMT factors, such as perceived severity, self-efficacy, and perceived vulnerability/susceptibility significantly influence users to practice security behaviour (Posey, Roberts, Lowry & Hightower, 2014; Cheng et al., 2013; Claar & Johnson, 2012; Vance et al., 2012).

Rational Choice Theory (RCT) is another theory that has been adapted by researchers to determine policy compliance behaviour and explain how individuals make decisions when faced with choices (Bulgurcu, Cavusoglu & Benbasat, 2010a). Bulgurcu et al. (2010a) also argued that an individual determines how he/she will act by balancing the costs and benefits of his/her options. RCT, which was originally developed by Becker (1968), suggests that offenders offset the costs and benefits of deviant behaviour in deciding whether or not to offend (Li, Zhang & Sarathy, 2010).

Bulgurcu et al. (2010a) described the process of rational decision-making in three stages. Firstly, an individual will recognize several alternative courses of action. Then, he/she will carefully observe the outcome of that action. Lastly, he/she will make a decision based on his/her perception of the costs and benefits of that action. Employees in the organization have the biggest impact on computer security because they are actually exposed to security threats when they are visiting related websites and downloading non-work related software (Li et al., 2010). The decisions made by employees towards the action that they take are critical. Therefore, organizations should enforce security policies because employees are less likely to commit deviant activities when the risk of getting caught and severity of punishment increases (Son, 2011).

Technology Threat Avoidance Theory (TTAT) was proposed by Liang and Xue (2009) and has been applied in IS studies related to technology threats. This theory explains the importance of understanding information technology threat avoidance behaviour among users. TTAT suggests that perceived effectiveness, perceived cost, and self-efficacy constructs can influence user information technology threat awareness (Rho & Ryu, 2011). If users are aware of IT threats, they will try to avoid any risk behaviour that can harm their job positions. Apart from that, TTAT also suggests that to motivate users to avoid malicious behaviour, they must perceive the effectiveness of using security-countermeasures and the confidence to use it properly. This can be helpful if users have knowledge concerning information security threats. The results found by Mejias (2012) stated that knowledge of a malicious IT threat is positively associated with information security awareness. If users have adequate knowledge of IT threats, their awareness towards information security would increase, and thus, conversely the risk of information security incidents would decrease.

Meanwhile, the ***General Deterrence Theory (GDT)*** focuses on deterrence or sanctions against deviant behaviour and suggests that when punishment of deviant behaviour is high and the sanctions are severe, potential criminals will be deterred from the perpetration of illegal acts (Theoharidou et al., 2005). Other literature explains that GDT emphasizes that punishment that is implemented by the authorities, such as the organization or lawmakers, is able to change people's behaviour (Ugrin & Odom, 2010). Individuals who are scared to be punished or shamed by getting caught due to deviant behaviour are less likely to commit any deviant activities in the organization (Son, 2011).

GDT is a theory that is mainly adapted in computer security studies based on two main constructs: (i) technical deterrence, which refers to the use of IS security software, and (ii) non-technical deterrence, which implements ISPs and guidelines. These two constructs have been shown to be important predictors of IS security deterrents (Al-Omari et al., 2012a; D'Arcy, Hovav & Galletta, 2009; Straub, 1990). Previous literature also integrated GDT and PMT in computer security studies (Herath & Rao, 2009a; Seppo et al., 2007) with the results showing that deterrence factors can influence user behaviour towards information security. This is supported by a recent research that stated that procedural security countermeasures or technical security countermeasures are a deterrent mechanism that can discourage employees from illicit behaviours (Hovav & D'Arcy, 2012).

Technology Acceptance Model (TAM) is adapted from the Theory of Reasoned Action (TRA) and has been applied in many studies to investigate user intention to use IS. TAM is a well-known model based on two fundamental beliefs: perceived usefulness (PU), and perceived ease of use (PEOU) (Davis, 1989; Egea & Gonzalez, 2011), to determine users' attitude and behavioural intention to use the system, as shown in Figure 2.7.

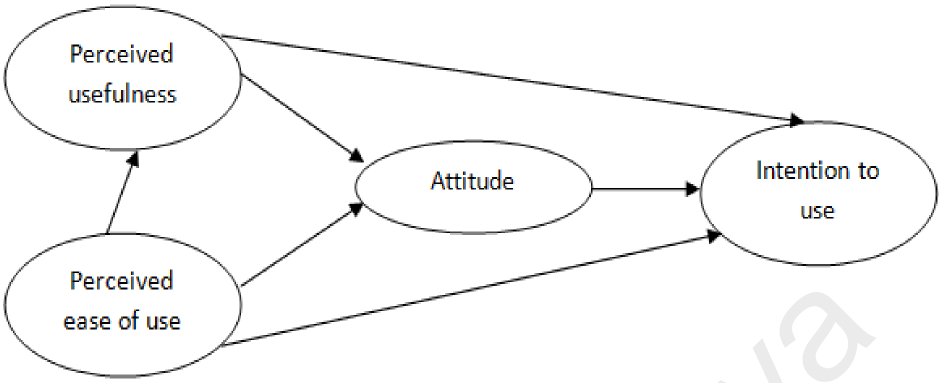


Figure 2.7: Technology Acceptance Model (Davis, 1989)

PU relates to the users' belief that the use of technology will enhance their job performance, whereas PEOU refers to how the user believes that using a particular system will reduce their effort and time (Davis, 1989). TAM has been widely used in studies related to e-commerce (Kim, Ferrin & Rao, 2008) and e-learning systems (Shen, Laffey, Lin, & Huang, 2006). Previous studies have shown that PU and PEOU contribute to users' behaviour towards IS acceptance (Kim, Tao, Shin & Kim, 2010; Kim et al., 2008; Shen et al., 2006). Al-Omari et al. (2012b) adapted the TAM model in their study to investigate user compliance behaviour towards ISPs. The study found that both PU and PEOU influenced users to comply with an organization's ISPs.

Users will have an intention to adopt the security technology if IS security is useful, easy to use and if they feel that the technology will increase their work performance (Al-Omari et al., 2012b). Security technology is an important element in IS development, and thus, it can be one of the factors that influences users to comply with the organization's ISPs. Security technology is a method to prevent information security threats, both internal and external. Thus, many organizations have invested a huge amount of money to implement the IS security using advanced technological tools, such as smartcards and biometrics (Guo, 2012). However, these tools are only good in preventing the external threats, and not internal threats (Doherty, Leonidas & Heather, 2011). In addition, ‘passwords’ as one of the commonly used methods are well known for their flaws due to user behaviour (Parsons et al, 2014; Vu et al., 2007). For example, many users fail to use strong passwords, resulting in low security protection. Most of them also hardly update their anti-virus software or scan their computers regularly. Workman, Bommer and Straub (2008) stated that most employees feel that security technology is tedious and time-consuming. Therefore, they usually fail to comply with the ISPs, and as a result, the vulnerability of the organization’s data is increased. Based on the literature, the current study suggests that the management of the organization should invest more cost in humans rather than technology alone in combating information security threats because if humans do not adopt the technology properly, information security incidents will still occur (Warkentin et al., 2011; Beas & Salanova, 2006).

Human behaviour always plays an important role in ensuring that organizational information can be protected and secured (Akhunzada et al., 2015; Parsons et al., 2014; Hagen, Albrechtsen & Hovden, 2008). When an organization implements security technology, it must consider the user perspective. Users who are unfamiliar with the technology may find it complicated, and thus, they will avoid using it. If on the other hand they feel that the security technology is easy to understand they may be encouraged to behave appropriately towards information security. Therefore, it is important to inject security awareness of security technology among employees in the organization through the implementation of security training and programmes.

Theory of Planned Behaviour (TPB) is another human behaviour theory that proposed by Ajzen (1985). TPB that has been applied extensively to examine users' acceptance of information systems, which is designed to predict human behaviour (Liao, Chen & Yen, 2007). This theory has also been adapted in other areas of study relating to regulations pertaining to the compliance behaviour among people (Poulter, Chapman, Bibby, Clarke & Chundall, 2008; Seppo et al., 2007). TPB postulates three conceptually independent determinants of intention: attitude, subjective norms and perceived behavioural control (Ajzen, 1991). Ajzen defined attitude as a *"degree to which a person has a favorable or unfavorable evaluation or appraisal of the behaviour in question".*Meanwhile, subejective norm refers to to the perceived social pressure and perceived behavioural control (PBC) is defined as the perceived ease or difficulty of performing the behaviour. As a general rule, the more favorable the attitude and subjective norm with respect to behaviour, and the greater the PCB, the stronger should be the person's intention to perform adequate behaviour (Ajzen, 1991).

Huang and Chuang (2007) defines subjective norms (SN) as users' perceptions of other people's opinions in terms of whether or not they should adopt appropriate behaviours. Other people's opinions in this context are the opinions of superiors and colleagues. However, in this study, the researchers have only highlighted the behaviour of superiors because the behaviour of employees in organizations is mostly influenced by their superiors, who are also the leaders in the organization, such as directors, managers or supervisors. This is because people tend to abide by what they have been told to do and to show respect for their superior, which can have a positive or negative effect (Leach, 2003). This is supported by previous findings, which have indicated that the behaviour of superiors has the most impact on employees' information security behaviour (Ifinedo, 2012; Huang & Chuang, 2007;). Leaders should show positive security behaviour and encourage employees' to comply with ISPs (Siponen et al., 2010) so that an adequate security culture can be inculcated in the organizations.

Meanwhile, PBC also can be described as users' perceptions of their ability (Huang et al., 2011), which can be heightened through education and training provided by the management. The PBC construct suggested by Taylor and Todd (1995) has two components: Self-Efficacy and Facilitating Condition. Self-efficacy actually originates from the SCT, which determines how people feel, think, and what motivates them to behave in a certain way based on cognitive, motivational, affective, social influence, and selection processes (Workman et al., 2008). An author of a previous study related to the self-efficacy of users with their confidence to use IS (Brady, 2011). According to Chan et al. (2005), people's self-efficacy can be developed through the ongoing acquisition of knowledge. This is agreed by previous researchers, in that the self-efficacy of users can be enhanced through training programmes provided by the management in the organization (Beas & Salanova, 2006). Self-efficacy towards information security influence not only involves the proper use of security-countermeasure tools, but also the security care behaviours related to computers or Internet usage.

Meanwhile, the facilitating condition is related to the facilities that are needed to ensure that employees engage in a behaviour that is required of them by the organization, such as money, time and other specialized resources (Taylor & Todd, 1995). In this study, the researchers focused on other resources that organizations should provide to enhance the abilities and skills of employees, such as in implementing security mechanisms and security training, which aims to monitor and educate employees to behave appropriately towards information security. Education and training programmes can develop users' information security awareness (Puhakainen, 2006) and enhance the users' skills to use security tools (Koskosas et al., 2011), which would lead to the improvement of users' compliance behaviour with ISPs. Figure 2.8 illustrates the basic TPB model.

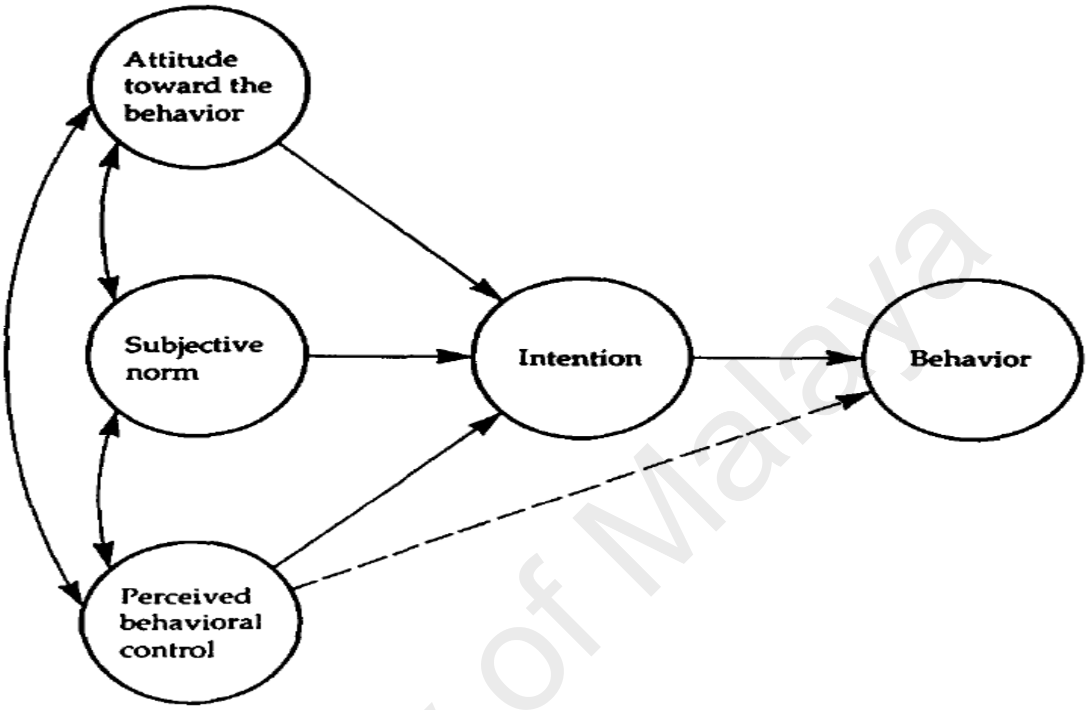


Figure 2.8: Theory of Planned Behaviour (Ajzen, 1991)

2.8 Justifications of Theories Adaptation

Based on the theory reviews, it has been shown that the theories have been adapted to many areas of studies such as sociology (Şimşekoğlu & Lajunen, 2008), health (Delgado, Norby, Dean, McIntosh & Scott, 2012; Lee & Gould, 2012) and IS (Ifinedo, 2012) to study human behaviour. These theories have been applied to examine ISPs compliance behaviour in an organization, for example PMT (Vance et al., 2012; Johnston & Warkentin, 2010; Workman et al., 2010), GDT (Cheng et al., 2013; Hovav & D' Arcy, 2012), TPB (Al-Omari et al, 2013; Cavallari, 2011), HBM (Ng et al., 2009), among others. Many previous studies focused on fear-based mechanisms, i.e. the fear of formal sanctions and threats to organization’s security (Cheng et al., 2013; Barlow et al., 2013; Hovav & D’ Arcy, 2012; Vance et al., 2012; Johnston & Warkentin, 2010; Li et al., 2010; Seppo et al., 2007). Most previous studies have focused on behaviour towards information security among employees in an organization; however, to the best of researcher knowledge, only few were conducted to assess the HIS security compliance behaviour among healthcare professionals (Noor Hafizah Hassan & Zuraini Ismail, 2012; Gathan Narayana Samy et al., 2009) while none of the studies investigated the mediation effect of information security awareness, particularly with respect to the relationship between management support and employee compliance behaviour towards ISPs.

Furthermore, studies on human factors such as trust and security barriers in relation to information security behaviour have not been explored much. Trust in organization ISPs can improve compliancy while barriers impeding compliancy with ISPs causes non-compliant behaviour among employees (Brady, 2011). Therefore, the current study aims to adapt two theories – HBM and TPB – as both theories consist of a number of constructs that have been widely used in various studies to explain human behaviour. Thus, the research objective one is to develop a research model by adapting two theories – TPB and HBM – and terming it as the Health Information System Security Policies Compliance (HISSPC) model. The current study assumes the adapted theories can increase the understanding of human behaviour in complying with an organization’s ISP by focusing on two dimensions: management support and information security awareness.

In this study, HBM constructs, such as perceived susceptibility, perceived severity and perceived benefit of security-countermeasures, are adapted as constructs of information security awareness, while perceived barriers as another construct. The current study is based on the stance that if users are aware of the severity of security incidents, they would behave with more caution (Bulgurcu et al., 2009; Workman et al., 2008). The greater the user awareness of information threats, the greater their awareness of its susceptibility, consequently leading to a reduction in security incidents. It is believed that when users are aware of the benefits of implementing an information protection mechanism over information assets to prevent threats that outweigh the cost of eliminating them later, they are more likely to enact proper security measures, and vice versa (Workman et al., 2008). Evaluation of secure behaviour is also affected by barriers, thus if a threat is perceived and secure behaviour is practised, then users would behave and handle the threat as recommended (Davinson & Sillence, 2010).

HBM was chosen because it consists of a number of constructs that are not represented in the adoption of Information Systems (IS) and other related theories, but is vital for information security practices (Ng et al., 2009). Moreover, HBM is able to measure or predict human behaviour successfully (Brown, Ottney, & Nguyen, 2011). This study focuses on the protective security behaviour of end-users, which is defined as behaviour that does not violate organizational security policies. These behaviours include the choice of a strong password, regular backing up of data and scanning of files or documents downloaded from emails or websites. Previous studies argue that these behaviours require IS users to consciously decide to perform actions for the sake of preventing security threats, such as loss of data to reduce the likelihood of security incidents (Shropshire et al., 2015; Ifinedo, 2014; Ng et al., 2009). For this reason, HBM is appropriately adopted in this study.

Meanwhile, TPB is well known as a significant model used to describe user behaviour in the application of IS (Fishbein & Ajzen, 1975). Moreover, TPB may well explain an individual’s cognition-based conscious behavior. However, it is noted that

TPB may not be appropriate for understanding habitual behaviour. According to TPB, human behaviour can be motivated by what other people think a person should do (Sun, Guo, Wang & Sun, 2006; Ajzen, 1991). With this in mind, this study emphasizes leader behaviour in motivating their followers to adopt proper security behaviour. TPB also explains that human behaviour is motivated by their perception of their ability to behave in a certain manner (Huang, Rau, Salvendy, Gao & Zhou, 2011).

It is vital for the management to give full commitment and support to their employees as end-users of IS concerning best practices for information security behaviour. Such top-level involvement can influence user awareness concerning information security. This is also emphasized by authors from previous studies who found that management plays an important role in encouraging positive user behaviour towards the use of IS (Ng et al., 2009; Yap, Soh & Raman, 1992). Top management must possess definite knowledge concerning the importance of information security to create an organizational environment that is conducive to achieve security goals. Studies have suggested that if the employers can provide a set of clear security guidelines and strictly monitor their employees, information security compliance will in turn increase (Herath & Rao, 2009a).

Among common reasons cited for the weak implementation of ISPs in organizations are lack of management support as they ought to, lack of authority, and lack of understanding on the importance of information security (Brady, 2011). It is essential that top management play their supportive roles well to ensure the effectiveness of IS security through their leadership behaviour. Additionally, management support is equally imperative for the implementation of ISPs, provision for sufficient information security training and the running of effective security awareness programmes for employees. Based on reviews, the TPB concept was adapted by placing leadership behaviour (SN), cues to action, information security training, as well as implementation of ISPs (PBC) as indicators of the level of management support.

Based on the review of the literature, other human factors important in information security are self-efficacy and trust. Self-efficacy is one of the main components of the PBC construct from TPB and has also been integrated in HBM. According to Brady (2011), self-efficacy is related to users' confidence to use IS. Meanwhile, Chan et al. (2005) argued that people's self-efficacy can be developed through the ongoing acquisition of knowledge. This is in agreement with previous researchers that self-efficacy of users can indeed be enhanced through training programmes provided by management in an organization (Rhee et al., 2009, Beas & Salanova, 2006;).

On the basis of trust, this study specifically adopts the trust construct. This study postulates that the adaptation of these theories and the trust construct can aid in the understanding of user compliance behaviour towards an organization's ISP. Thus far, the trust factor has not been explored with detail in studies concerning information security compliance behaviour although the trust factor has been shown to be one of critical importance in IS (Kim et al., 2008). This is also argued by Williams (2008), who found that a trustful environment is significant in influencing information security practices particularly with respect to insider threats. Therefore, trust should be explored in-depth in investigating the information security compliance behaviour of employees and also be added in the HISSPC model.

2.9 Trends of Information Security Studies

In the early days, many IS studies were focused on information security technology (Theoharidou et al., 2005, Evans & Yen, 2005; Fry & Dann, 2002) and privacy issues (Gathan Narayanan Samy e al., 2009; Eric & Goetz, 2007). However, numerous studies reported that the main information security threat in an organization is internal threat from employees (Safa et al., 2016; Siponen et al., 2014; Ng et al., 2009). These employees have legitimate and often privileged access to facilities and organizational information, knowledge of the organization and its processes and know the location of critical or valuable assets (Colwill, 2009). With this in mind, many organizations now realize the need to invest not only in the technical aspects of the system, but also in the human resource aspect. The current trend in IS security studies also emphasize employees' compliance behaviour towards ISPs implemented in the organization (Lee, Lee, & Kim, 2016; Safa et al., 2015; Siponen et al., 2014;, Barlow et al., 2013; Vance et al., 2012) as shown in Figure 2.9. Many researchers argued that the effectiveness of IS security can be achieved if IS users practice adequate information security behaviour and comply with the security policies and procedures implemented in the organization (Safa et al. 2016; Warkentin et al., 2011; Li et al., 2010).

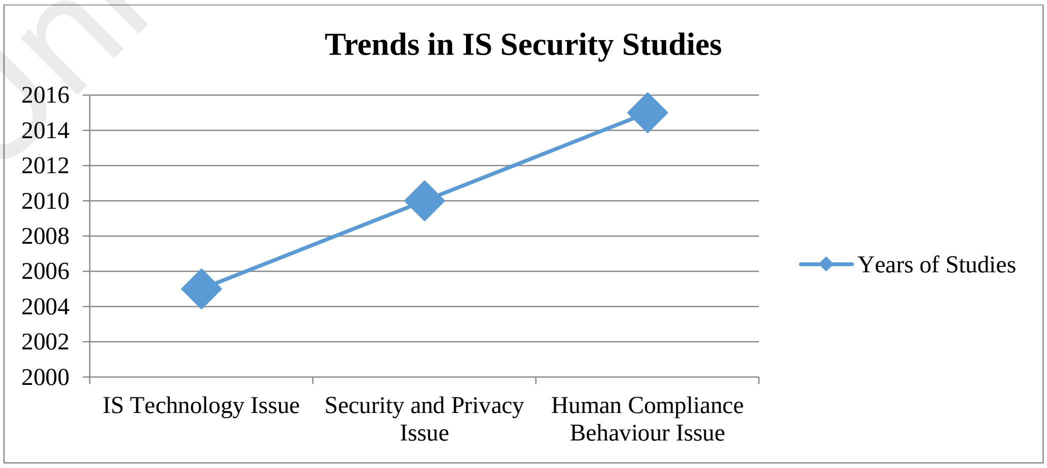


Figure 2.9: Trends in IS security studies

Many empirical studies on compliance behaviour towards ISPs have been done in Western countries such as the United States of America and Finland in which most of their respondents were from industries such as the banking industry (Al-Omari et al., 2012b; Bulgurcu et al., 2010a; Myyry et al., 2009). In Malaysia, the healthcare industry already implements electronic patient records, upgrades and Intranets for sharing information among related healthcare providers and utilizes the Internet to distribute health related information. HIS helps healthcare industry to manage the administrative, financial and clinical aspects of hospitals (Nurul Izzatty Ismail et al., 2013). Moreover, HIS has a higher degree of vulnerability towards the threats of information security such as unauthorized access, use, disclosure, disruption, modification or destruction and duplication of passwords. This could be a result of greater openness to multi-connected systems of heterogeneous stakeholders within the network. Therefore, ISPs compliance behaviour among healthcare professionals is important.

Previous studies have argued that ISPs are important because they provide a set of rules and procedures that help define the recommended information security levels in an organization that employees should follow (Yildirim et al., 2011). These policies also highlight the importance of information security aspects, such as how to protect valuable information (Knapp et al., 2009) and help to reduce the number of security incidences in an organization (Kruger & Kearney, 2006). However, security incidents cannot be reduced if information security behaviour among employees cannot be improved, especially if they are not aware of the existence of ISPs. Thus, information security awareness among employees is very important in organizations because of its capability to reduce the occurrence of security incidents (Al-Omari et al., 2012a; Eminağaoğlu et al., 2009).

Previous studies stated that management play a vital role in enhancing employees' awareness concerning information security (Al-Omari et al., 2012a; Choi, Kim, Goo & Whitmore, 2008; D'Arcy et al., 2009). These studies suggested that the information security awareness could be improved through preventative efforts by top management, such as implementing information security training programmes. The authors of previous studies also reported that employees who receive security training present secure behaviour (Barlow et al., 2013; Hovav & D'Arcy, 2012; Jenkins, Durcikova & Burns, 2012) and are more likely to comply with the organization's ISPs (Ifinedo, 2012). Hu et al. (2012) stated that management can make a difference with respect to security behaviour. This can be done through building up a security culture in the organization (Da Veiga & Martins, 2015). Leaders in the organization should show positive security behaviour and encourage their employees to attend any information security training and strictly enforce their employees to follow any security policies and rules implemented in the organization (Safa et al., 2015).

Human factor is also a major contributor to information security behaviour, in that human perception towards information security threats can affect information security compliance behaviour (Safa et al, 2016; Siponen et al., 2010; Herath & Rao, 2009b). Furthermore, self-efficacy and security policy barriers are also determinants of security behaviour (Ng et al., 2009; Rhee et al., 2009). The summary of empirical findings of related studies is presented in detail in Table 2.5.

Table 2.5: Summary of previous empirical research in ISPs compliance behaviour

Authors	Theory/Model	Sample	Summary of Research Findings
(Safa et al., 2016)	Social Bond Theory Involvement Theory	296 employees from four different companies (Retail/Wholesale, IT company, Education and Government) in Malaysia	Information security knowledge, colloborations, security experience, user's commitment, and personal norms are significant on employees' attitude towards compliance with organizational ISPs.
(Safa et al., 2015)	TPB PMT	Information security experts and IT professionals in Malaysia organizations.	Information security awareness, information security policy, information security experience and involvement, attitude towards information security, subjective norms, threat appraisals, and information security self-efficacy have a positive effect on user's behavior.
(Siponen et al., 2014)	PMT	669 employees from various Finnish corporations.	Perceived severity, perceived vulnerability, attitude and social norms towards complying with ISPs had a significant effect on employees' intention to comply with ISPs.
(Al-Omari et al., 2013)	Based on TPB to construct Security Ethical Model (SEM)	445 employees in Jordan Bank industry	Awareness and training have an impact on secure behaviour. Attitude, subjective norms, ethical, and self-efficacy are significant to intention to comply with ISPs.
(Cheng et al., 2013)	Deterrence Social theory	185 employees	When employees are aware of the severity of sanctions, they can make a conscious decision to perform secure behaviour.

Authors	Theory/Model	Sample	Summary of Research Findings
			The relationship between management and employees is important.
(Barlow et al., 2013)	Neutralization Deterrence	257 employees in US Company.	Training and awareness can reduce security policy violations. Some dimensions of neutralization have a significant impact on the intention to violate the security policy.
(Hovav & D'Arcy, 2012)	Deterrence	US – 269 Korea –145	User moral belief can be enhanced through training and security programmes. Severity of punishment has an impact on the security behaviour among users.
(Al-Omari et al., 2012a)	Based on TAM to construct Security Awareness Model.	205 Bank employees	Subjective norms, PU, and PEOU are significant to predict intention compliance behaviour. Self-efficacy, controllability and information security awareness (ISA) influence PU and PEOU.
(Vance et al., 2012)	PMT Habits theory	54 security experts and IT managers	All PMT constructs are significant, except vulnerability. Habit has an important role in compliance behaviour. Role of management to spread security message.

Authors	Theory/Model	Sample	Summary of Research Findings
(Mejias, 2012)	TPB TAM Unified theory	208 healthcare professionals in US hospitals.	Organizational support and self-efficacy lead to HIPPA compliance.
(Waly et al., 2012)	TRA TPB Organizational factor	360 employees	Organizational communication, sanctions, and rewards are significant. Awareness and strong motivation are required.
(Jenkins et al., 2012)	Learning and media theory	238 students	Users who receive training exhibit higher secure behaviour.
(Hu et al., 2012)	TPB Organizational factor Culture	148 employees in US Company.	Management can make a difference with respect to security behaviour. Building security culture is significant.
(Ifinedo, 2012)	PMT TPB	76 employees	Attitude, behaviour of superiors, social pressure, self-efficacy, threat appraisal, and response efficacy are significant on ISPs compliance behaviour intention. Compliance behaviour can be increased if management provides security awareness programme, training and campaigns.
(Son, 2011)	Motivation: Intrinsic and extrinsic factor	602 employees in US Company.	Intrinsic motivation is significant, but extrinsic is less significant on compliance behaviour. Security training is important to enhance employee security behaviour.

Authors	Theory/Model	Sample	Summary of Research Findings
(Brady, 2011)	Organizational factor Culture	76 healthcare staff in US hospitals.	Management support culture and security awareness are significant for security behaviour and its effectiveness.
(Yoshikai et al., 2011)	Virtual game	100 users	Users with high experience and high media skills influence protective behaviour.
(Cavallari, 2011)	Culture TPB	213 employees in Europe.	Workplace culture has a positive impact on attitude and compliance security behaviour. Superior behaviour influences employee’s behaviour.
(Bulgurcu et al., 2010a)	TPB RCT	464 research employees in US Company.	ISPs compliance influenced by attitude, normative belief, and self-efficacy. ISA effects belief and compliance behaviour. Awareness programme and training can ensure employee’s ISA and develop self-efficacy.
(Johnston & Warkentin, 2010)	Extensions of PMT	275 academic staff and students in US higher education.	Response efficacy and self-efficacy strongly influence user compliance behaviour. Social slightly influences user compliance behaviour. Threat appraisal is not significant.
(Puhakainen & Siponen, 2010)	Theory based learning	16 employees	Training programme is important. Visible support of IS security by management is necessary to ensure users comply with ISPs.

Authors	Theory/Model	Sample	Summary of Research Findings
(Li et al., 2010)	Rational Choice Theory	246 employees	Employees are more likely to comply with security policies when perceived behaviour is overridden by potential risks from formal sanction and security threats. Organizational factors indirectly influence intention compliance behaviour.
(Wang, 2010)	TAM	220 respondents	User attitude and intention can be a predictor of security behaviour. Users' knowledge is related to intention towards adopting secure behaviour.
(Siponen et al., 2010)	PMT Deterrence TRA	917 employees	Threat appraisal, SE, NB, and visibility of the intention to comply with ISPs are significant. ISA can prevent security incidents. Training, awareness programmes and campaigns can increase ISA. Management plays an important role in promoting security behaviour among employees.
(Rhee et al., 2009)	Extended SCT	415 graduate students in the US	Individuals with higher self-efficacy use more security software than low self-efficacy. Self-efficacy influences security care behaviour. People's belief in their self-efficacy can be influenced by learning and social persuasion.

Authors	Theory/Model	Sample	Summary of Research Findings
(Ng et al., 2009)	Extended HBM	134 employees	Perceived susceptibility, perceived benefit, and self-efficacy are determinants of computer security behaviour. Perceived severity moderates the effects of perceived benefit, security orientation, cues to action, and self-efficacy on computer security behaviour. Users did not find many barriers in practicing safe behaviour.
(Herath & Rao, 2009b)	PMT Deterrence TPB	312 employees in US Company.	Employees who understand the severity of the threat significantly affects their concern regarding security breaches. If employees believe that complying with policies is difficult, they are less likely to comply. Management communication is important. Resource availability can enhance self-efficacy. Social is significant.
(Zhang, Reithel, & Li, 2009)	TPB Technical security protection	176 employees in US Company.	Perceived behavioural control and attitude are significant on intention to comply with ISPs. If users feel that their compliance with ISPs are favourable, they are more likely to comply. Subjective norms are insignificant.

Authors	Theory/Model	Sample	Summary of Research Findings
(Workman et al., 2008)	PMT	588 respondents	People consistently implement security measures if they perceive the security threat as severe. All factors under PMT are significant.
(Seppo et al., 2007)	GDT PMT TRA IS Security and etc.	240 respondents	The quality of ISPs has a significant effect on actual security behaviour. Attitude, NB, and NH are significant on intention to comply with ISPs.

Based on previous empirical findings as shown in Table 2.5, this study has highlighted several constructs (Information security awareness, management role, self-efficacy and trust) that need to be investigated further to get more understanding on user's compliance behaviour towards ISPs.

2.9.1 Information Security Awareness

Information security awareness refers to the understanding of employees concerning the importance of information security, ability to recognise information security threats and their responsibility to practice security behaviour properly to protect an organization's data (Shaw et al., 2009; Rezgui & Marks, 2008). Bulgurcu et al. (2009) defined information security awareness as employees' general knowledge about information security and their consciousness of the organization's ISPs. Wang (2010) argued that security awareness and experience are part of an individual's security knowledge. If employees have little knowledge concerning information security, they might not be aware of the importance of complying with and practicing the organization's ISPs. Additionally, Boss et al. (2009) stated that in order for an employee to follow security policies and procedures, an employee should be generally aware of security threats. Information security awareness among employees should not just cover only on the general knowledge of security awareness, but employees should have knowledge and awareness on the severity and susceptibility of security threats as well as the benefits of security tools that can be used to mitigate the security threats.

Bulgurcu et al. (2010a) proposed integration models (TPB and Rational Choice Theory) to investigate the compliance behaviour of employees in US professional market research companies. Their research model also included the role of information security awareness in employee compliance or non-compliance with the ISPs, and argued that information security awareness can encourage compliance behaviour among employees. In another empirical finding, it was found that proper awareness towards information security among employees can have an impact on their behaviour (Kreicberga, 2010). Human error and problematic behaviour can be reduced if an employee's security awareness is increased (Parsons et al, 2014; Shaw et al., 2009). Therefore, organizations should make information security awareness among employees a top priority by organizing information security training and awareness programmes (Cheng et al., 2013). Information security training and awareness programmes should be established properly because they can help to refresh employee knowledge. This is also argued by Straub (1990), who stated that employee's awareness can be improved through communication of formal ISPs, which is in this case referring to the formal security training and programme. Safa et al. (2015) also stated that the security awareness programmes should be relevant and consistent because both are the key to success in information security awareness.

Moreover, Kreicberga (2010) stated that employees' knowledge and their experience can also be developed based on the behaviour of their superiors and other co-workers. Thus, the management must give full support and build a positive environment in the organization to ensure that all employees adhere to the organization's rules and regulations through information security awareness programme. For example, in healthcare environment, information sharing is part of how health information is being delivered; but, it allows the visibility and flow of health information exposed among people which has to be controlled and monitored by the management to ensure the information will not be misused. In this case, information security awareness among employees is necessary.

2.9.2 The Role of the Management to Increase Information Security Awareness among Employees

The full support from the management in any organization is essential as it can ensure information system security effectiveness, and enables the creation of secure environments for information handling (Safa et al., 2015; Hu et al., 2012; Brady, 2011;). Management support refers to the commitment from the management in the organization as observed by employees (Al-Salihy et al., 2003; Chan et al., 2005). In the security context, this commitment refers to documenting organization ISPs, ensuring that policies and procedures are put into practice in an organization, and providing security training and awareness programmes (Knapp et al., 2009; Johnston & Warkentin, 2008). According to Kankanhalli, Teo, Tan, and Wei (2003), management support is considered as a form of guidance provided during IS security planning and implementation.

Management support is still in its infancy in information security studies, with most previous studies focusing on security technology (Brady, 2011; Santos, Correia, & Antunes, 2008). However, some empirical studies have shown that management support is important, for example, Johnston and Warkentin (2008) combined organizational and individual factors based on TPB and TAM to determine the compliance intention behaviour of healthcare professionals with the Health Insurance Portability and Accountability Act (HIPPA) in the US. Their findings showed that management support plays a role in healthcare professional compliance intention behaviour as well as self-efficacy. Brady (2011) revealed that management support is a significant predictor of security behaviour of healthcare professionals in the US towards HIPPA. Meanwhile, Al-Salihy et al. (2003) adapted the IS security effectiveness model, and found that management support did not significantly influence IS security effectiveness.

As discussed earlier, management can show their support for information security behaviour through organizing and developing information security training, awareness programmes and the implementation of ISPs. Information security training, awareness programmes and ISPs implementation are the methods to inform employees about organizational ISPs (Koskosas et al., 2011; Martin & Rice, 2001), which aim to introduce and provide information about the importance of using security countermeasures to avert information security threats and the impact of this threat to the organization. In addition, the management should ensure that the contents of ISPs during training and awareness programmes clearly outline employee responsibilities, define authorised and unauthorised uses of the systems, procedures to report suspected threats to the system, define penalties for violations and provide a mechanism for updating the ISPs (Whitman, 2004).

The ISPs cannot be implemented effectively if the employees do not know or aware about it. Thus, it is necessary that the ISPs are correctly and appropriately deployed throughout the organization and actually brought to all employees (Höne & Eloff, 2002). According to Hone and Eloff (2002), the distribution of ISPs can be done during information security training using full paper based or electronic copies of the documents, through publishing the document on internal website. It is also can be deployed during an awareness session, which gives the opportunity to reinforce and explain the message of the policy immediately to the employees. Information security training can overcome information security awareness issues as it has been reported that information security training is one of the security mechanisms that can influence employee information security awareness (Jenkins et al., 2012; Hagen et al., 2008). In addition, information security training is also able to improve an employee’s skills towards using security tools properly that can prevent security threats (Liang & Xue, 2009; Beas & Salanova, 2006; Torkzadeh & Van Dyke, 2002). It is believed that information security training and awareness programmes demonstrated management support.

The researchers in past studies have suggested that organizations should invest more in human capital instead of technology itself. This is because most of the security incidents are caused by the carelessness, negligence, and lack of capability of internal employees in using security tools properly (Akhunzada et al., 2015; Parsons et al., 2014; Koskosas et al., 2011; Park et al., 2010). Furthermore, many security incidents reported in previous studies are caused by internal employees due to a lack of security awareness (Al-Omari et al., 2013; Aurigemma & Panko, 2012; Albrechtsen & Hovden, 2010; Brady, 2010; Herath & Rao, 2009b). Therefore, the management should conduct information security training for all employees in the organization. Training is an effective tool to ensure that users have the right attitude towards information security, which can reduce the number of security incidents (Al-Omari et al., 2012b; Jenkins et al., 2012).

According to Eminağaoğlu et al. (2009), security training is a powerful mechanism for mitigating information security risks. However, security training should be conducted regularly because human beings tend to forget what they have learnt. Thus, it is vital for organizations to conduct ongoing security trainings to ensure that employees are always aware of the importance of information security (Hagen et al., 2008). Additionally, appropriate security training for employees is important because it can create and maintain a high level of information security awareness (Ifinedo, 2012; Bulgurcu et al., 2009; Puhakainen, 2006). A recent study also suggested that security awareness training is effective for decreasing violations against an organization's ISPs (Barlow et al., 2013). Therefore, effective security training should be able to deliver messages about information security risks to all employees and teach them how to utilize IS security practices properly.

Furthermore, according to Abdul Rahman Ahlan et al. (2011), a lack of information security awareness among employees occurs because they do not fully understand the importance of their organization information, and hence, employees give less priority to information security. In addition, the management should inculcate good security behaviour in all employees and make information security awareness the first priority in the development of ISPs. Through effective training and education, employee behaviour and information security skills may be improved as employees are encouraged to have good information security practices as recommended by their organizations (Rezgui & Marks, 2008).

Meanwhile, the authors of other studies argued that security awareness programmes or campaigns affect the compliance behaviour of employees towards information security (Albrechtsen & Hovden, 2010; Yoshikai et al., 2011; Eminağaoğlu et al., 2009). Security awareness programmes or campaigns have been reported as the best way to increase employee awareness because the security message can reach employees efficiently (Rezgui & Marks, 2008). The implementation of information security training and security awareness programmes is the responsibility of the management. The management should seriously consider and give full support to this issue to ensure that employee security behaviour is acceptable. The content of information security training and security awareness programmes should cover detailed information about security threats, as well as the severity with which these threats can spread through organizations (Siponen et al., 2010). In addition, information security messages must be delivered effectively through security awareness programmes and the management must always alert their employees to the seriousness of internal threats through emails or messages, as it is an appropriate cue to encourage the desired information security behaviour.

The behaviour of superiors in this study focuses on employees' perception towards their leaders on how the leaders monitor and control the employees so as to ensure that they are aware of the organization's ISPs. The characteristics of leaders to monitor and control their followers is referring to leadership style (Zhen, Yuqiang & Qing, 2012; Aaron, 2006; Burns, 1978). Many leadership studies have shown that leadership styles have a significant influence on an employee's work performance (Aurigemma & Panko, 2012; Kaushal, 2011; Lo, Ramayah & Run, 2010; Yukl, 2008). Strong leadership is required in guiding users to make the right decisions and to promote information security awareness among users.

According to Abdul Rahman Ahlan et al. (2011), leadership skills are essential in the creation of a basis for security awareness, and it has been argued that leadership has an impact on employee awareness concerning the importance of complying with an organization's ISPs. The behaviour of employees in organizations is mostly influenced by their superiors who are leaders in the organization, such as directors, managers and supervisors. This is because people tend to follow what they have been told to do and show respect to their superiors, which can have a positive or negative effect (Leach, 2003). This is supported by other research that also found that the behaviour of superiors has a significant effect on the intention of employees to comply with the organization's ISPs (Ifinedo, 2012; Kyobe, 2010; Hagen et al., 2008; Wiant, 2005).

In the current study, two types of leadership style were explored: transformational and transactional. The transformational leadership style is a leader who motivates and encourages his/her subordinates to think critically and creatively, which can influence employees' commitment in the organization (Avolio & Bass, 1988), while the transactional leadership style is a leader who motivates his/her subordinates through reward and punishment (Wang, Tsui, & Xin, 2011). This type of leader strictly monitors the employees' activities. Sometimes, security training and security awareness programmes may not be effective; therefore, the management should control and monitor employee behaviour by ensuring that all employees adhere to ISPs. They do not just monitor and control employee behaviour, but also show positive security behaviour. This is argued by Griffin and Hu (2013), who stated that leaders set an example of right and wrong behaviours, which provides a sign that helps employees to determine appropriate action or behaviour. Moreover, most of the employees will not believe in organization's ISPs if they do not see their leaders conforming to, and living by it (Höne & Eloff, 2002). In fact, the security behaviour should be practiced by all levels of the organization to ensure the effectiveness of ISPs.

Information security awareness concerns the degree of employees' understanding towards information security threats, which can affect the organizational process and also their understanding towards the importance of conducting information security behaviour to prevent information security threats (Abdul Rahman Ahlan et al., 2011). Employees should be aware of the probability of information security threats that may exist in the organization (perceived susceptibility) and the consequences of information security threats to the employees and organization (perceived severity) if the threat exists (Mejias, 2012). Employees must be able to identify information security threats (Thomson & von Solms, 2006) so that they would be able to adjust their action. However, this action is based on their decision, and employees make decisions based on their understanding of the subject (Kruger & Kearney, 2006). Previous studies have argued that if employees are not aware of their security actions, it may result in many IS security incidents (Cheng et al., 2013). Therefore, the management play an important role in injecting the right knowledge about information security to all employees by conducting information security training and education, and implementing security awareness programmes or campaigns effectively.

Johnston and Warkentin (2010) investigated the influence of threat appraisal on the compliance behaviour of employees who are the end-users of an organization’s IS using PMT. According to the results of their analysis, threat appraisal (perceived severity and perceived vulnerability) is a predictor of employee behaviour towards compliance with an organization’s ISPs. In other empirical studies, it has been argued that employees who are aware of the consequences of non-compliance behaviour, such as loss of job and severe penalty, will be more careful and adopt acceptable security behaviour as recommended by the organizations (Vance et al., 2012; Siponen et al., 2010; Herath & Rao, 2009b; Seppo et al., 2007). If an employee’s perception concerning damage or danger increases, it would lead them to behave appropriately towards information security. Otherwise, if they perceived that a risk has diminished, they would behave in a less cautious manner (Workman et al., 2008).

Gurung, Luo, & Liao (2008) adapted the perceived severity to evaluate maladaptive behaviour and the consequences of not adopting security behaviour. Their analysis indicated that if users’ perceptions towards threat severity were high, then they would be more likely to adopt security behaviour. The findings of this study were based on a study in security behaviour and the use of anti-spyware software. Moreover, they also argued that security education is important to raise spyware risk awareness among users. Similar research has been done, in which both threat appraisal (perceived severity and perceived vulnerability) significantly influenced users to adopt spyware security tools (Chenoweth et al., 2009). Users may be aware of the importance of using security tools, but they lack the skills in using it, which leads to behaviour based on ignorance. Thus, the users need to be properly trained.

The research conducted by Crossler (2010) indicated that perceived vulnerability and perceived severity were negatively significant when applied to computer security behaviour, such as backing up files. Meanwhile, Ng et al. (2009) found that perceived susceptibility significantly affected users to adopt computer security behaviour, such as scanning files using anti-virus software when downloading them from emails, while perceived severity had no effect. This is different from the analysis of Lwin et al. (2011), which showed that perceived severity affected protection behaviour against online harassment, while perceived susceptibility was insignificant. They also suggested that security programmes should emphasize the severity of security threats and effectively train all users in how to conduct security behaviour appropriately. This is also supported by Siponen et al. (2010) who argued that security education should be provided by the management and conducted by the IT staff, and inferred that the employees should be aware of security threats and the severity with which the threats can spread throughout the organization.

The research findings of Siponen et al. (2010) indicated that perceived severity and perceived susceptibility significantly affected users' compliance behaviour towards the organization's ISPs. They also argued that non-compliance behaviour with ISPs would be reduced if the management strictly enforced security penalties, such as work suspensions or discharge. The management must also ensure that their employees are able to recognize information security threats and the risks that these threats can pose to the organization (Vance et al., 2012). Otherwise, if employees do not believe that they or the organization would be subjected to information security threats, they would be unlikely to comply with the ISPs (Ifinedo, 2012). Moreover, ISPs that are implemented by the organization must be easy to understand and applied by all categories of employees – novice or expert users.

The research findings by Li et al. (2010) indicated that employee intention, when complying with security policies, involves cost-benefit analysis. According to them, employees are more likely to comply with security policies when perceived benefits are overridden by the potential risk of formal sanctions and security threats. Furthermore, Vance et al. (2012) highlighted that employees must recognize information security threat and the risk these threats pose to their organizations. Based on this awareness, they might comply with ISPs and practice good security behaviour. However, employee compliance behaviour towards ISPs might reduce if they feel that following the security policies is time consuming and slows down their work (Hagen et al., 2008). This situation happens when employees have to work under pressure, such as the need to submit their work tasks within a short time (Siponen et al., 2010). On the other hand employees are likely to practice computer security behaviour if they perceive the effectiveness of adopting computer security tools (Ng et al., 2009). Based on the above reviews, the management should emphasize the benefits of using security-countermeasures to prevent information security threats during training and education sessions because it can help employees to be more responsible (Eminağaoğlu et al., 2009).

Even though the management gives full support to information security by organizing security training and implementing advanced security technology, if employees are still unaware and do not care about the importance of practicing information security behaviour, the security objectives will not be achieved. Bearing this issue in mind, this study believes that information security awareness can mediate the relationship between the management support and employee compliance behaviour towards ISPs.

2.9.3 Self-Efficacy

In information security studies, self-efficacy is defined as an individual’s belief in their capability to protect information from threats, such as unauthorized disclosure, modification, and loss (Rhee et al., 2009). Ng et al. (2009) defined self-efficacy as a person’s self-confidence to perform a particular behaviour. In health information privacy studies, self-efficacy is defined as an individual’s perception towards the capability to protect patient information privacy (Johnston & Warkentin, 2008). According to SCT, people with greater confidence are more likely to initiate challenging behaviours (Rimal, 2000; Siwei & Xiaoping, 2009). Rhee et al. (2009) argued that people with high self-efficacy are likely to focus their attention on analysing and formulating solutions to problems, whereas people with low self-efficacy tend to engage in fewer coping efforts. They also argued that self-efficacy towards information security influence is not only about the use of security tools or software, but that security behaviour is also related to computer usage, as well as Internet usage. For example, people with high self-efficacy will use more security software, make backup copies, use strong passwords and are more alert to security threats.

Self-efficacy has been widely used to examine employee’s compliance behaviour towards the organization’s ISPs. Previous studies indicated that self-efficacy has a significant effect on an employee’s intention to comply with the organization’s ISPs (Son, 2011; Bulgurcu et al., 2010a; Herath & Rao, 2009b), and that compliant behaviour towards ISPs can be promoted by increasing self-efficacy (Chan et al., 2005). This is also supported by Seppo et al. (2007), who indicated that self-efficacy was significant in explaining people’s adherence to information system security. Employees are more likely to adopt their organization’s ISPs if they have the relevant competence and capability with regard to taking information security precautions and to implement preventative security measures (Ifinedo, 2012).

The authors of previous research also found that self-efficacy is one of the important constructs in determining information security practices (Rhee et al., 2009) and to have positively influenced employees' compliance behaviour towards information security (Brady, 2011). Self-efficacy is significantly related to other computer security behaviour, such as adopting anti-spyware (Gurung et al., 2008) and using anti-virus software to scan any files downloaded from an email (Ng et al., 2009).

Many studies have reported that most of the security incidents are caused by the incapability of internal employees in using security tools properly (Koskosas et al., 2011; Park et al., 2010). Therefore, organizations should conduct information security training for all their employees. Training is an effective tool for educating users in how to use security tools properly and ensuring that users have the right attitude towards information security, which can reduce the number of security incidents (Al-Omari et al., 2012b; Jenkins et al., 2012). Appropriate security training for employees is important because it can create and maintain a high level of information security awareness and increase self-efficacy (Puhakainen, 2006). The information technology staff who organize security training should also be able to deliver messages about information security risks effectively to all employees and teach them how to utilize IS security practices properly.

2.9.4 Trust

Trust has a variety of definitions according to the background of the study. In terms of the psychological aspect, trust is defined as the willingness of an individual (a trustor) to accept vulnerability to the action of another individual (a trustee) (McDermott, Conway, Rousseau, & Flood, 2013; Shahnawaz & Goswami, 2011), whereby an individual believes that he or she will not be taken advantage of by another individual (Six & Sorge, 2008). Trust is also defined as an individual's confidence in other people's honesty and beliefs (Crosby, Evans, & Cowles, 1990). Meanwhile, Rhee (2010) classified trust according to three dimensions: (i) social trust, which is reflected with social culture; (ii) organizational trust, which is defined as the degree of trustfulness of an organization (this concept of trust reflects the working rules and norms of work activities in the organization); and (iii) trust in others, which is the trust relationship between the co-workers and the employer.

According to Tan and Lim (2009), trust in an organization refers to an employee's willingness to be vulnerable to their organization's actions, which has been shown to be a significant factor for motivating an employee's commitment and thus increasing organizational performance (Hogler, Henle, & Gross, 2013; Celep & Yilmazturk, 2012). This is supported by Utami, Bangun, & Lantu (2014), who stated that it is important for the organization to gain the trust of employees in order to increase their commitment to work. Furthermore, Shahnawaz and Goswami (2011) argued that the trust factor is important in building human relationships, in this case, the relationship between the employee and the employer. If employees feel that they are treated well by their employer, they will work harder in return to achieve organizational goals, and as a result, their commitment to the organization increases (Celep & Yilmazturk, 2012; Brower, Lester, Korsgaard, & Dineen, 2009).

In information technology studies, trust is the basis of information security and privacy (Kim et al., 2008) and has been widely used in e-commerce research, particularly in defining how users feel about the security and their willingness to adopt it (Chung & Kwon, 2009). Previous empirical findings reported that trust positively affects the behaviour of consumers who intend to use online transactions (Chung & Kwon, 2009; Kim et al., 2010), and that it is a powerful predictor of information security behaviour among employees (Williams, 2008). Other areas of study in information technology also adapted perceived trust concerning issues related to information security and privacy (Kim et al., 2008) and provide similar definitions. In other contexts of computer science, trust is defined as the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible (Jøsang, Roslan Ismail & Boyd, 2007). Trust has also been defined as the security expectation of security policies from a service (Bahtiyar & Ufuk Çağlayan, 2012).

Trust is also a primary predictor of technology usage (Li, Hess &Valacich, 2008), however, although trust was not explored much in IS studies related to compliance behaviour it is still important in information security. It is believed that it is essential to maintain trustworthiness between employees and management of the organization to ensure that employees give full commitment by complying with organizational rules and policies to protect an organization's assets and data. This was argued by Nyhan (2000), who stated that, for trust to exist, employees and top management must be confident with each other, whereby both parties believe in each party's competency and will act in a fair and ethical manner. For example, the management should appreciate their employees through career promotion, and in return, employees will give extra effort towards job performance, in this case, by complying and practicing security behaviours appropriately.

Trust has also become an important factor in social relationships, that is, a lack of trust in certain situations among people will lead to lesser performance on social, as well as academic and professional levels (Dumortier & Vandezande, 2012). This is supported by previous research, which indicated that trust is important in increasing the commitment and loyalty among employees (Harvey, Reiche & Moeller, 2011). Thus, the relationship between management and employees should be positively built to ensure employees' commitment (Maley & Moeller, 2014).

Previous studies also suggested that the trust construct should be explored in studies related to information security compliance behaviour in medical centres as health data are sensitive and distributed among healthcare providers, such as doctors, hospital administration, laboratories and insurance companies (Bahtiyar & Ufuk Çağlayan, 2013; Brady, 2010). According to Bahtiyar and Ufuk Çağlayan (2013), even though an organization has implemented ISPs with the aim to reduce security incidents, it still requires the trustworthiness of ISPs among the employees. This is also argued by Kogler et al. (2013) who stated that an individual's compliance behaviour towards rules and regulations can be improved if fostered by the trustworthiness of policymakers.

In the healthcare environment, health professionals must give full commitment when dealing with health data (Brady, 2010), especially when the data can be accessed through a network that is vulnerable and poses a risk to it (van Deursen et al., 2013). The possible security risks, among others, include staff sharing passwords to access health data, leaving the computers without logging out and staff emailing health data to the wrong addressee, thus disclosing patient data to an unauthorized user. Moreover, health data may be subjected to security and privacy attacks because the health information system that is implemented in the hospitals is connected to the Internet, which is vulnerable to security threats (Bahtiyar & Ufuk Çağlayan, 2013). The potential risks exist because of the lack of understanding of security concepts among health professionals, which fosters reliance on trust within the work environment instead of trust in a hospital's security policies (Williams, 2009).

The perception of trust among users depends on the subjective needs of the users and social constraints. If users have higher trust in the security system, they will likely use the security system consistently, which, in turn, may reduce security incidents in the organization (Bahtiyar & Ufuk Çağlayan, 2013). This is also supported by Lippert and Davis (2006) who stated that trust is an important element in the organization as trust affects an employee's willingness to adopt the security technology implemented in the organization. With this in mind, it is believed that trust in organizations should be embedded between the employees and the hospital management in the healthcare sector; thus, the employees will be more committed to comply with the information security policies implemented in the healthcare sector and security incidents can be decreased. Therefore, trust in the current study refers as HIS users expected confidence on the implementation of HIS security policies through managerial support.

2.9.5 Perceived Barrier

Perceived barrier in HBM refers to people's difficulty in adopting security behaviour (Ng et al., 2009). Perceived barrier is also known as the response cost in PMT, which refers to people's beliefs about how costly it is to perform the recommended behaviour (Herath & Rao, 2009b). In this study, the barrier to information security refers to the unskilled employees towards security technology due to their lack of security awareness.

In addition, previous literature has identified several key barriers in adopting security behaviour (Waly et al., 2012), such as lack of a clear role and the responsibility given to the employees, lack of incident reporting in the organization, lack of security recovery, and lack of security awareness. Meanwhile, Lee et al. (2011) referred to barriers as any cost related to taking adaptive action, such as monetary, time, effort, inconvenience and complexity. If people feel that to perform information security behaviour requires a lot of time and effort, then they will be less likely to perform information security requirements (Bulgurcu et al., 2009). Similarly, if employees feel that complying with an organization's ISPs are slowing down their work, then they will be less likely to perform compliance behaviour (Herath & Rao, 2009b). This happens because employees have to work under extreme pressure and hurry to finish their work (Hagen et al., 2008), especially in medical centres, where health professionals have to serve many patients almost every day.

Chenoweth et al. (2009) argued that user's perceptions concerning difficulty in using security software, such as anti-spyware, plays a key role in their decision to use it. Using PMT in their study, barriers to using security software was found to be negatively significant. Meanwhile, Ng et al. (2009) adapted HBM in their study and found that users did not find many barriers in practising safe email behaviour. Safe email behaviour is one example of computer security behaviour. Furthermore, the empirical findings of Vance et al. (2012) showed that employees did not find any difficulty with complying with security policies. However, it is still important to investigate perceived barrier, especially in a health institution environment, because barriers in practising security behaviour can be the reason why most of the employees do not comply with ISPs, as discussed above.

2.10 Gaps in the Literature

After reviewing the literature pertaining to the compliance behaviour of information security towards ISPs and the theories adapted from previous studies, four main gaps were identified, as shown in Figure 2.10.

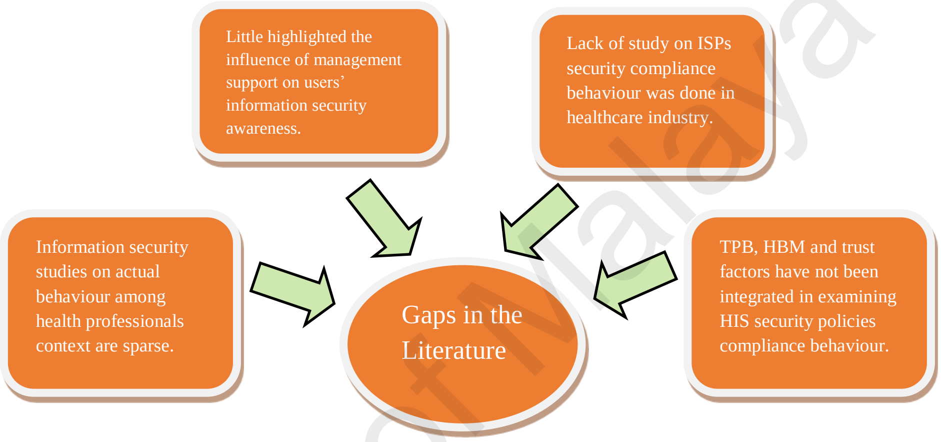

Little highlighted the influence of management support on users' information security awareness.
Lack of study on ISPs security compliance behaviour was done in healthcare industry.
Information security studies on actual behaviour among health professionals context are sparse.
Gaps in the Literature
TPB, HBM and trust factors have not been integrated in examining HIS security policies compliance behaviour.

Figure 2.10: Summary of gaps in the literature

Firstly, most of the studies investigated the effects of the human-technical factors on the intention behaviour rather than the actual behaviour. For example, in TPB, the central of factor is the individual's intention to perform a given behaviour. Taylor and Todd (1995) criticized TPB stating that the models require individuals to be motivated to perform certain behaviour; this assumption may be problematic when studying user's compliance behaviour, in addition to the assumption of an identical belief structure among respondents when it comes to performing security behaviour. Therefore, the current study adapts TPB with other theory and concept, which focus on management support, employees' information security awareness and self-efficacy into consideration. It is believed that these factors are the determinants of information security behaviour. In addition, this study explores the effects of the following constructs: trust in the organization and security barrier on compliance behaviour towards ISPs. Additionally, the researcher linked the constructs with the actual behaviours of end-users, because if their behaviours are monitored, it can provide a more accurate indication of the effectiveness of health information system security.

Secondly, although previous studies have discussed information security behaviour, to the best of the researcher's knowledge, none of the previous studies have been conducted to assess the indirect effect of management support on ISPs compliance behaviour through health professional information security awareness and self-efficacy in the health institution, and the direct effect of perceived trust. People who are attached to an organization are the ones who use the technology; thus without proper knowledge of information security and lack of trustworthiness concerning the organization's ISPs, they will not be able to utilize security behaviour appropriately. Therefore, this study has developed a new model by considering all the indicated factors to investigate users' compliance behaviour towards ISPs.

Thirdly, almost all of the studies on ISPs compliancy behaviour were carried out in Western countries, in which most of the respondents were staff working in industrial companies, such as banking and retail. The current study has moved the frontier to investigate compliancy behaviour towards ISPs in healthcare industry in Malaysia, with respondents who are health professionals working in government hospitals. Lack of study in ISPs compliance behaviour focus on health professionals, especially in Malaysia, the implementation of HIS is just a new beginner. Therefore, it is important to explore health professional's compliance behaviour towards HIS security policies before the full version of HIS being implemented in the hospitals. HIS plays a major role in planning, initiating, organizing, and controlling the operations of the subsystems of the hospitals (Aniza Ismail et al., 2010). Thus, information security behaviour among health users should be seriously considered

Finally, the majority of the empirical studies employed several behaviour models adapted from, among others, the PMT (Ifinedo, 2012; Herath & Rao, 2009b;), TPB (Warkentin et al., 2011; Bulgurcu et al., 2010a; Siponen et al., 2010), Rational Choice Theory (Bulgurcu et al., 2010a; Li et al., 2010) and Deterrence Theory (Herath & Rao, 2009b; Straub, 1990). Only one study (Ng et al., 2009) has been found to employ HBM to investigate employee security behaviour. In the current study, TPB and HBM were adapted to develop a HISSPC model because both theories are widely known in human behaviour studies in the domains of health and information security.

HBM is a comprehensive healthcare theory because it consists of a number of constructs that are not represented in information system (IS) adoption or other theories, but are important in IS security (Ng et al., 2009). Previous studies showed that HBM is a relevant theory to be adapted in IS security studies because the characteristics of preventive health care (such as observing a healthy diet to avoid bad diseases) and protective behaviour (such as using a strong password to prevent unauthorised access) are similar (Ifinedo, 2012; Ng et al., 2009). The difference between the studies is that one is used to reduce the effect of diseases, while the other is used to reduce the risk of security incidents.

Meanwhile, TPB is the most significant model used to explain user behaviour in IS studies (Uffen & Breitner, 2013; Ifinedo, 2012). Since the current study focuses on management support (superior behaviour, security training, programmes, and implementation of ISPs), information security awareness (awareness of threat susceptibility, threat severity and benefit of security-countermeasure), self-efficacy and perceived barrier, the adaptation of the TPB and HBM is applicable in this study.

Additionally, trust is another human factor that should be explored as trust in the organization's ISPs can improve compliancy with ISPs among employees (Brady, 2011). Hence, this study is believes that the integration model provides a detailed theory of human behaviour, which is valuable for understanding compliance behaviour in respect of the information security policies in the Malaysian healthcare environment.

Figure 2.11 shows the proposed research model that explains the link between the theories and constructs adapted in this study.

2.11 Health Information System Security Policies Compliance (HISSPC) Model

The Health Information System Security Policies Compliance (HISSPC) model consists of three exogenous constructs (management support, perceived barriers and perceived trust). Management support consists of leadership behaviour, cues to action as well as information security policies training and education. Information security awareness and self-efficacy were adapted as mediators. Information security awareness consists of three intervening constructs (perceived benefit, perceived susceptibility and perceived severity). Moreover, HIS usage experience was posited as a moderator and the endogenous construct in the current study is HIS security policies compliance behaviour, as shown in Figure 2.11.

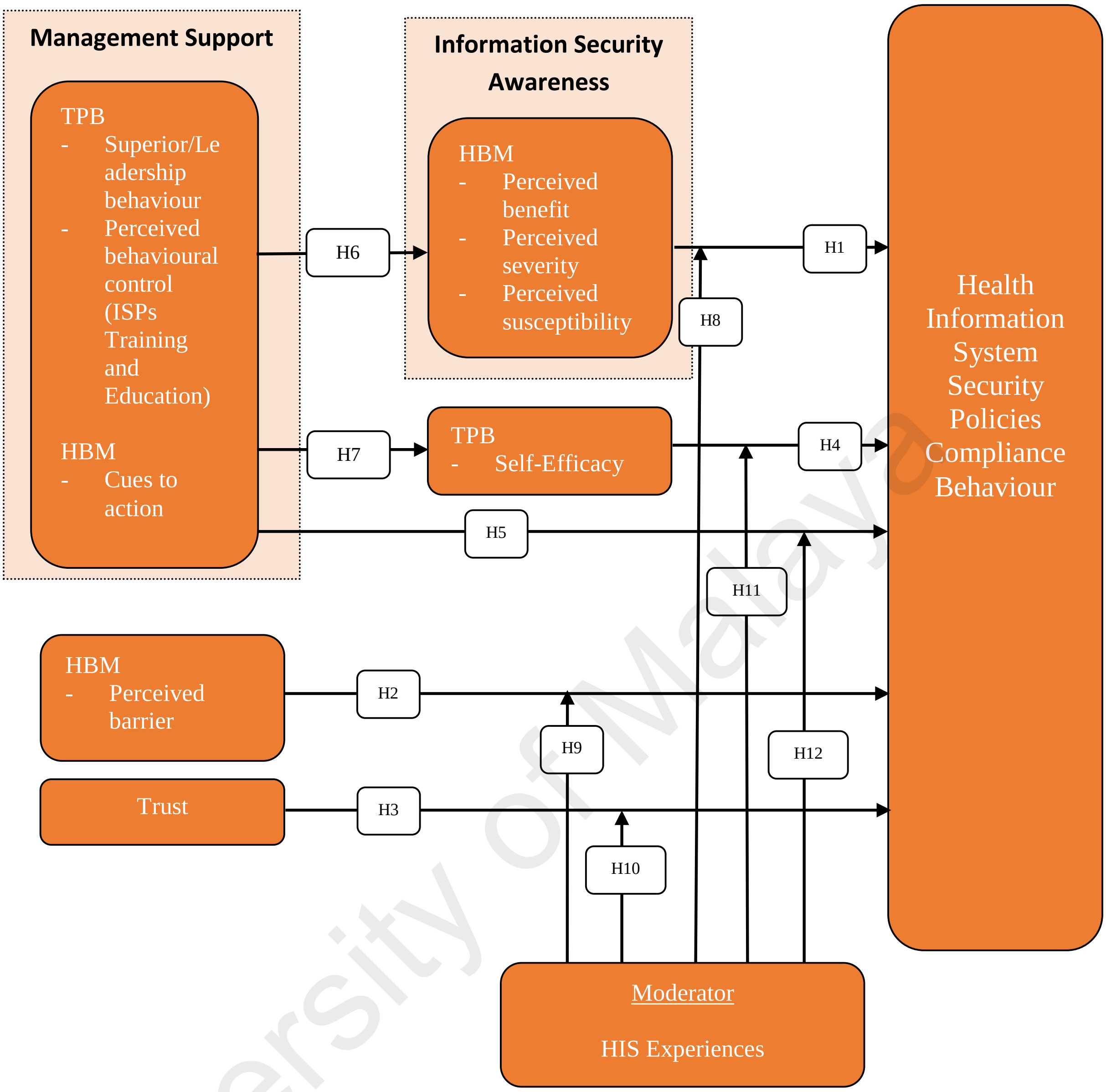

Management Support
TPB
- Superior/Leadership behaviour
- Perceived behavioural control (ISPs Training and Education)
HBM
- Cues to action
Information Security Awareness
HBM
- Perceived benefit
- Perceived severity
- Perceived susceptibility
TPB
- Self-Efficacy
HBM
- Perceived barrier
Trust
H1
H2
H3
H4
H5
H6
H7
H8
H9
H10
H11
H12
Moderator
HIS Experiences
Health Information System Security Policies Compliance Behaviour

Figure 2.11: HISSPC Model

2.11.1 An Effect of Information Security Awareness on Users' Compliance Behaviour towards HIS Security Policies

The rapid rise of threats from viruses, worms and the like, has illustrated the need for increased awareness among users. Bulgurcu et al. (2010a) defined information security awareness as an employee's general knowledge about information security and his/her cognizance of the ISPs in the organization. Information security awareness is an important factor as it can ensure that users are aware of security risks and practice the recommended security behaviour (Rezgui & Marks, 2008). Previous studies found that many employees have low user awareness and understanding of information security (Brady, 2011; Da Veiga & Eloff, 2010), and that it is one of the critical information security components (Kim, 2014; Al-Omari et al., 2012a;). In the current study, three constructs taken from HBM were grouped under information security awareness, as follows:

Perceived benefit is defined as the degree to which a person perceives the positive outcomes of performing certain secure behaviour, such as using security-countermeasures adequately (Bylund et al., 2011). The researcher believes that when people are aware of the benefits of implementing information protection mechanisms and information assets outweigh the cost of protecting them, they are more likely to enact security practices, and vice versa (Workman et al., 2008). Thus, the following hypothesis was derived:

H1(a)*: Perceived benefit will have a positive effect on HIS security policies compliance behavior.*

On the other hand, ***perceived severity*** is defined as users' perceptions on the seriousness of potential damages or threats (Bulgurcu et al., 2009; Ng et al., 2009). According to Kruger et al. (2011), the information security threats may result in huge losses of data if there is limited realization on the fraudulent acquisition of sensitive information. Many empirical studies reported that the perceived severity of security incidents causes people to behave in a more cautious manner if their degree of perception of the potential damage or danger increases (Bulgurcu et al., 2009; Workman et al., 2008). Based on this, the following hypothesis was constructed:

***H1(b)**: Perceived severity will have a positive effect on HIS security policies compliance behavior.*

Meanwhile, perceived susceptibility classified as the subjective risks assessment on information threats (Woon & Kankanhalli, 2007). The number of information security incidents can be reduced if employees are aware of the risk of information security threats to health data. If high susceptibility is perceived by employees, they will be motivated to adopt information security behaviours (Younghwa, 2011). Thus, the following hypothesis was constructed:

***H1(c)**: Perceived susceptibility will have a positive effect on HIS security policies compliance behavior.*

2.11.2 An Effect of Perceived Barrier, Trust and Self-Efficacy on Users' Compliance Behaviour towards HIS Security Policies

Ng et al. (2009) defined ***perceived barrier*** as users' expected distortion of practicing information security behaviour. According to Ng et al. (2009), the barriers to information security are the reason for not practicing computer security in their workplaces. Several barriers that reduce the need of people to engage in healthy eating behaviour were identified, such as lack of knowledge, lack of self-control and lack of time. Similarly, perceived barrier may be the reason why employees do not try to practice computer security in their work. Therefore, the current study posits the construct as one of the predictors for determining users' behaviour towards information security and the following hypothesis was constructed:

***H2**: Perceived barrier will have a negative effect on HIS security policies compliance behavior.*

In this study, ***trust*** refers to users expected confidence on the implementation of security policies through managerial support. The trust of health professionals' in the management of health institutions will enhance their compliance behaviour with ISPs related to HIS use. Therefore, perceived trust is considered as one of the constructs that can affect users' compliance behaviour towards HIS policies and the following hypothesis was developed:

***H3**: Trust will have a positive effect on HIS security policies compliance behavior.*

Social Cognitive theory defined ***self-efficacy*** as a social dimension of human capability (Johnston & Warkentin, 2008; Bandura, 1989;). Heterogeneous agents with a higher level of self efficacy have utilized motivation, cognitive resources, collections of actions, organizational support to execute goals of organization (Workman et al., 2008) through persistent efforts (Bandura, 1989). With general features of self-efficacy, computer self-efficacy (CSE) was developed by Davis (1989) and Gist et al. (1989). It refers to subjective judgement of one's cognitive capability in dealing with computer usability. It has received multidimensional attentions from various scholars who have examined human-computer interactions such as information system (Compeau & Higgins, 1995; Ellen, Bearden, & Sharma, 1991; Venkatesh, Morris, Davis, & Davis, 2003), ethical computer usage (Kuo & Hsu, 2001), and development of systems (Hunton & Beeler, 1997). It has supported positive acquisition of skills (Beas & Salanova, 2006; Chan et al., 2005) among health professionals in dealing with compliance behaviour towards HIS security of policies.Thus, the following hypothesis was constructed:

***H4**: Self-efficacy will have a positive effect on HIS security policies compliance behavior.*

2.11.3 An Effect of Management Support on Information Security Awareness and Users' Compliance Behaviour towards HIS Security Policies

Management Support is described as the users' perception of the commitment of top management to protect information; an aspect that is one of the critical security components (Da Veiga & Eloff, 2010). In the current study, management support is measured based on social pressures and organizational resources.

Social Pressures

The behavioural literature has recognized the significance of social pressures in the organization. The social pressures in TPB are called subjective norms, which can be defined as the views of those people who are important to an employee that will affect the employee's behaviour (Siponen et al., 2010). The following construct indicates social pressures:

This study relates superior behaviour with ***leadership behaviour***, which is defines as a style of leadership focusing on how a leader monitors and controls the employees to ensure that they will comply with ISPs. One technique to convince employees to comply with information security policies is to receive social pressure from their leaders. Foremost, the leaders should show positive security behaviour by obeying all the security rules and policies (Siponen et al., 2010). In addition, leaders can share their knowledge about information security with employees, which will encourage the employees to practice information security behaviour properly. This has been outlined by a previous study in which leader behaviour was found to have the most impact on employees' information security behaviour (Herath & Rao, 2009a). Thus, it is essential that leaders show a positive attitude towards information security.

In the current study, two leadership styles were adapted to measure leadership behaviour. The leadership styles were transformational leadership and transactional leadership. Leaders who are engaged with their team members and motivate them are said to have the characteristics of a transformational leader (Burns, 1978), whereas a transactional leader is one who operates within the existing system or culture and strictly controls how the system is implemented in the organization (Bass, 1985). Many leadership studies have shown that both leadership styles are significantly influential on employees' work performance (Kaushal, 2011; Lo et al., 2010). Strong leadership is required to guide users in making the right decision and to comply with ISPs. Previous literature argued that leadership is able to influence employees or end-users of IS in the organization to follow rules and procedures, and guide them in making the right decision (Aaron, 2006). Therefore, the following hypotheses were highlighted:

H5(a)*: Leadership behaviour will have a positive effect on HIS security policies compliance behavior.*

H6(a-i)*: Leadership behaviour will have a positive effect on perceived benefit.*

H6(a-ii)*: Leadership behaviour will have a positive effect on perceived severity.*

H6(a-iii)*: Leadership behaviour will have a positive effect on perceived susceptibility.*

Resources

Besides monitoring and controlling employees, management must also consider and be aware of employees' information security skills, because they contribute to the success of an organization. This can be achieved through information security training, which aims to introduce and provide information about the importance of an information system's security. Information security training also increases the users' skill and understanding towards information security as indicated by PCB. The effectiveness of an information system's security can be achieved if users are aware of the importance of practicing information security. Well-managed security training can educate employees to comply with ISPs, and therefore, management must ensure that the security training in their organizations is conducted efficiently. The following constructs indicate the resources of the employee's development:

Cues to action is defined as users' experience concerning security threats, which can encourage and activate them to practice computer security (Ng et al., 2009). Basically, users will experience and obtain information about security incidents through security awareness programmes, media cues, social influences and recommendations from security experts (Meillier, Lund & Kok, 1997). In health research, cues to action were reported to have a significant effect on the behaviour of individuals (Hanson & Benedict, 2002; Ross et al., 2010). Information security messages must be delivered effectively through security awareness programmes and the management must always alert their employees to the seriousness of internal threats. This can be done through emails or messages, which are an adequate cue to encourage the desired information security behaviour. Therefore, this construct must be considered, as it is believed to influence employees to practice information security behaviour; hence, the following hypotheses were constructed:

***H5(b)**: Cues to action will have a positive effect on HIS security policies compliance behaviour.*

***H6(b-i)**: Cues to action will have a positive effect on perceived benefit.*

***H6(b-ii)**: Cues to action will have a positive effect on perceived severity.*

***H6(b-iii)**: Cues to action will have a positive effect on perceived susceptibility.*

Information security policies training and education is a programme that aims to introduce and provide information about the importance of security systems, with which all employees should comply. Information security awareness can be achieved through the security training of employees, as training is one of the methods to deliver an organization's ISPs (Koskosas et al., 2011). Well-managed security training can educate employees to comply with ISPs. Therefore, management must ensure that their organizations have implemented security training effectively.

On the other hand, it is important that organizations provide proper documentation of ISPs that employees can understand and practice. The current study believes that with a well-documented and clear explanation of ISPs, users' awareness concerning information security can be increased and security incidents in an organization can be decreased. If the information security policy is easy to understand, can be adopted easily and definitely not too strict, it will increase users' awareness, and thus, encourage users to behave appropriately in respect of information security. Gunson et al. (2011) argued that if security processes are difficult to use, users will avoid them and will fail to use them properly. For example, in order to create a highly secure password, several text characters and numbers need to be combined, which makes it difficult for users to remember the passwords.

The current study believes that if the management monitors HIS users efficiently and provides effective information security programmes and training, users will be more aware of the benefits of security-countermeasures, as well as the susceptibility and severity of information threats. Thus, they are able to comply with and practice information security policies properly, leading to a reduction in the number of security incidents. Based on the review above, the following hypotheses were developed:

H5(c)*: Information security policies training and education will have a positive effect on HIS security policies compliance behaviour.*

H6(c-i)*: Information security policies training and education will have a positive effect on perceived benefit.*

H6(c-ii)*: Information security policies training and education will have a positive effect on perceived severity.*

H6(c-iii)*: Information security policies training and education will have a positive effect on perceived susceptibility.*

2.11.4 An Indirect Effect of Management Support on Users' Compliance Behaviour towards HIS Security Policies through Information Security Awareness and Self-Efficacy

In the current study, it is believed that the relationship between management support and users' compliance behaviour towards ISPs can mediate through the information security awareness dimension based on these three constructs: awareness of benefit of security-countermeasures (perceived benefit), awareness of the consequences of not practicing and complying with ISPs (perceived severity) and awareness of the susceptibility of an organization's data (perceived susceptibility). On the other hand, the mediating effect of management support on ISPs compliance behaviour through employees' security skill is also possible.

Management constitute employees' compliance behaviour towards ISPs (Brady, 2011) and employees' compliance behaviour indicates the effectiveness of the IS security that is implemented in the organization (Al-Salihy et al., 2003). Employees' compliance behaviour can be improved if their awareness of information security is high (Albrechtsen & Hovden, 2010). The information security awareness in the current study consists of employees' awareness of the probability of a security threat occurring in the organization, and the seriousness of the security threat to the employees and organization if it occurred. Additionally, if employees are aware of the benefit of using security-countermeasures, it can also help to reduce security incidents.

It is believed that if the management monitors employees efficiently and provides effective information security programmes and training, they will be more aware of the benefits of security-countermeasures as well as the susceptibility and severity of the information threats. Thus, they are able to comply with and practice information security policies properly, leading to a reduction in the number of security incidents.

Thus, this makes the current study believe that there is a possibility of an indirect effect between management support and ISPs compliance behaviour through the extent of perceived benefit, perceived severity and perceived susceptibility. Therefore, the mediating hypotheses were constructed as follows:

H6(d-i)*: Leadership behavior will have a positive indirect effect on HIS security policies compliance behaviour through perceived benefit.*

H6(d-ii)*: Leadership behaviour will have a positive indirect effect on HIS security policies compliance behaviour through perceived severity.*

H6(d-iii)*: Leadership behaviour will have a positive indirect effect on HIS security policies compliance behaviour through perceived susceptibility.*

H6(e-i)*: Cues to action will have a positive indirect effect on HIS security policies compliance behaviour through perceived benefit.*

H6(e-ii)*: Cues to action will have a positive indirect effect on HIS security policies compliance behaviour through perceived severity.*

H6(e-iii)*: Cues to action will have a positive indirect effect on HIS security policies compliance behaviour through perceived susceptibility.*

H6(f-i)*: Information security policies training and education will have a positive indirect effect on HIS security policies compliance behaviour through perceived benefit.*

H6(f-ii)*: Information security policies training and education will have a positive indirect effect on HIS security policies compliance behaviour through perceived severity.*

***H6(f-iii)**: Information security policies training and education will have a positive indirect effect on HIS security policies compliance behaviour through perceived susceptibility.*

Besides monitoring and controlling the employees, the management must be aware of employees' information security skills. Self-efficacy in the current study is related to employee's information security skills, which is defined as users' perception about their computer security skills that can motivate them to behave in a certain way. Self-efficacy can be enhanced through information security awareness programmes and training, which aim to introduce and provide information about the importance of information system's security and to increase users' skill in using security-countermeasures (Torkzadeh & Van Dyke, 2002). Users might be aware of information security threats and have a good knowledge about security-countermeasures, but, if they have low skills in performing them, then they will be less likely to implement preventative security measures (Workman et al., 2008). Thus, management must educate employees concerning how to use security-countermeasures properly and why maintaining security behaviour is effective in preventing information security threats. Users' skill towards using security-countermeasures is also believed to mediate the effect of management support on ISPs compliance behaviour. Thus, the following hypotheses were developed:

***H7(a)**: Leadership behaviour will have a positive effect on self-efficacy.*

***H7(b)**: Cues to action will have a positive effect on self-efficacy.*

***H7(c)**: Information security policies training and education will have a positive effect on self-efficacy.*

***H7(d)**: Leadership behaviour will have a positive indirect effect on HIS security policies compliance behaviour through self-efficacy.*

***H7(e)**: Cues to action will have a positive indirect effect on HIS security policies compliance behaviour through self-efficacy.*

***H7(f)**: Information security policies training and education will have a positive indirect effect on HIS security policies compliance behaviour through self-efficacy.*

2.11.5 Health Information System's (HIS) Experience as a Moderator

Experience is related to individual abilities, knowledge and skills, which are developed through formal or informal education (Van Maele & Van Houtte, 2012). Shen et al. (2011) referred to experience as the knowledge or skills that people obtain through the involvement in or exposure to a particular event. The moderating effect of usage experience in information systems (IS) has been widely investigated in e-commerce studies, such as users' technology acceptance (Crespo, Salmones Sánchez & Bosque, 2013) and users' behavioural intention (Lin, 2011; Shen et al., 2011). Both of the previous studies have shown that users' experiences with IS moderate the effect of users' intention to use the technology. Therefore, HIS experience was posited as a moderator for the supplementary of the study.

This study considers users' experience at handling HIS to process health records as a moderator in the relationship of identified constructs and users' compliance behaviour with ISPs. Such experience includes experience with information security incidents, information security training and understanding the consequences of not complying with the policies relating to the HIS security policies. Benner (1984) stated that employee’s working experience with system environment in the same or similar situations may create competence. In this study, the respondents were divided into two groups based on the duration of users’ experience with HIS (moderating variable). Health professionals with durations of more than five years were classified to the group of higher experience users whilst those with less than five years were classified as lower experience users (McHugh & Lake, 2010). Based on the nature of Malaysian HIS, the experiences of health professionals are connected to the system usage.

Low experience employees was referred as new *born babies* who are new to the system and require *bottle feeding* from top management to understand the system environment quickly. Meanwhile, health professionals with high experience of HIS have gained recognitions through absorptive capacity in dealing with implicit features of security threats and speed of innovation to catch up on latest development and updates of tools to maintain effective protective records of health system.

Awareness on information security is an essential aspect of information management (Thomson, von Solms & Louw, 2006; Van Tassel, 1972). It ensures that all the employees are aware of their roles in securing the information (Parsons et al., 2014; Puhakainen, 2006). It has an additional role of monitoring the holistic evaluation of security mechanism via its predicted threats, and benefits among the users (Partridge, 2005; Parker, 1981). Health professionals with higher HIS experience are fully aware of the seriousness on the growing threats through higher absorptive capacity. Those with lower exposure need to have preliminary understanding of the severity (through information security training provided for them) to be consistent with system catch up.

Moreover, health professionals with higher HIS experience will be able to maintain compliance behaviour towards the designed security policies through innovation catch up with the latest developments on advanced security tools from various sources continuously and vice versa. This study believe that health professionals with higher HIS experience will stick to expansionary mode of perceived benefit since they are deal with higher levels of perceived susceptibility. With supporting lines of thoughts, this study suggests these hypotheses related with information security awareness:

H8(a): *High experience users significantly moderate the positive relationship between perceived benefits and compliance behaviour towards HIS security policies.*

H8(b)*: High experience users significantly moderate the positive relationship between perceived severity and compliance behaviour towards HIS security policies.*

H8(c)*: High experience users significantly moderate the positive relationship between perceived susceptibility and compliance behaviour towards HIS security policies.*

Experienced employees with proper knowledge can reduce the barrier of practicing ISPs, thus increasing the compliance behaviour. Additionally, high experienced health professionals of HIS perceive significant direction of technological barriers to avoid non-compliance behaviour compared to health professionals with lower system usability due to their innovation catch up. Therefore, this study suggests the following hypothesis:

H9*: High experience users significantly moderate the negative relationship between perceived barriers and compliance behaviour towards HIS security policies.*

Highly experienced health professionals know the ins and outs of the hospital's information system and they will be more committed to comply with the ISPs. Moreover, users with high experience will be able to deal with the future threats of security system although Blaze (1993) stated that transparent security system will be secure without the understanding of users on the technicality. Therefore, this hypothesis was formulated:

***H10**: High experience users significantly moderate the positive relationship between perceived trust and compliance behaviour towards HIS security policies.*

It has supported positive acquisition of skills (Beas & Salanova, 2006; Chan et al., 2005) among health professionals in dealing with compliance behaviour towards HIS security policies. Through the catch up effect, health professionals with greater system usage will acquire stronger acquisitions of security counter-measures (D'Arcy et al., 2009; Torkzadeh & Van Dyke, 2002) to comply with the innovative catch up of security policies. Therefore, this hypothesis was proposed:

***H11**: High experience users significantly moderate the positive relationship between self-efficacy and compliance behaviour towards HIS security policies.*

Leadership theory starts out with the realization of leaders (top managements) on security requirements in terms of costs, consequences, and guidelines within the organization. Through the scaled down version of inputs (Wilson & Hash, 2003), less experienced users will be able to utilize the given resources to comply with the security policies. Thus, this hypothesis was formulated:

***H12(a)**: Low experience users significantly moderate the positive relationship between leadership behaviour and compliance behaviour towards HIS security policies.*

The focus on the potential consequences of information governance is a culture of dual interactions between employees and security controls (Grant, 2005; Martins, 2002) such as passwords, access cards, anti-virus software and so on. Training by managing organization favours health professionals with lower exposure on HIS system. They require them to get to know the simpler version of technical features within the HIS system, including the security architecture to deal with compliance via system catch up rather than innovation catch up. It should be based on cost-effectiveness and ease of use (Wylder, 2004). Moreover, changes in existing policies and notification of security issues can be made to health professionals through emails, newsletters and articles effectively. Highly experienced health professionals may not need the technical support as they would be well exposed and capable of dealing with security policies independently. With this, this study formulates the following hypotheses:-

***H12(b)**: Low experience users significantly moderate the positive relationship between cues-to-action and compliance behaviour towards HIS security policies.*

***H12(c)**: Low experience users significantly moderate the positive relationship between information security policies training and education, and compliance behaviour towards HIS security policies.*

.

2.11.6 Dependent Construct - HIS Security Policies Compliance Behaviour

The multi-directional mindsets of compliance ascribes to non-technical aspects of deterrence theory. Herath and Rao (2009a) considered both internal (perceived value or perceived benefits) and external motivations (penalties, and social pressures) as the *relieving tonics* of security residuals. Chan et al. (2005) connected corporate structures (upper management practices) and perceived information security (perception of social climate and self efficacy) with compliant behaviour. Siponen et al. (2010) added on by reflecting on the significant factors, such as, normative beliefs, perceived severity, perceived susceptibility, self efficacy, response efficacy, visibility and deterrents to gage users contravene behaviour towards security system (Workman et al., 2008). D'Arcy and Hovav (2009) highlighted four promotional factors, namely awareness of security policies, monitoring, preventative software, and training to maintain the propensity of compliant behaviour.

The evolutionary dynamism of compliance serves multi-purposes such as monitoring of existing system architecture and design of preventative packages rather than just sticking to the retention of compliance behaviours among end users. Whitten and Tygar (1999) highlighted some conditional requirements for clients before the usability of security software:

(i) Users should be aware on the reliability of software before performing tasks of interest.

(ii) Users should know the successful steps of dealing with software.

(iii) Users should not make significant errors

(iv) Users should be comfortable with the features of software.

It is clear and evident that compliance behaviour towards the information security among clients can be symbolized as a linear function of intrinsic values and external environment. Although there are growing debates about it, there are limited evidences of factors to validate compliance behaviour among health professionals in the Malaysian context.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

The research methodology is the heart of the study that describes the detailed activities of the investigation being conducted. The research goal can only be accomplished if the research method is conceived and executed in such a manner that the data collected are accurate and directly relevant to the research problems stated in the previous chapter.

The methodology chapter in this thesis includes the research paradigm, research design, research framework, and the data collection procedures. These procedures describe the sampling frame, population, sampling technique and size, unit of analysis, research instrument, as well as the validity and reliability of the instrument. This chapter also explains the analysis procedure of the data and the development process of the health information system prototype.

3.2 Research Paradigm

Research is mainly based on one or more research paradigms. The research paradigm is viewed as a basic set of beliefs and assumptions that we are willing to make, that serves as a touchstone in guiding research activities, as explained by Guba and Lincoln in their work in 1989 (Saidon, 2012). According to Rubin and Babbie (1989, as cited by Mitra, 2000, p. 37), *"A paradigm is a fundamental model or scheme that organises our view of something. Although a paradigm does not necessarily answer important questions, it tells us where to look for the answers".* Mitra (2000) also states that when a theory is tested, and a research problem is solved, and it is applicable in a similar context, it becomes a paradigm.

The research paradigm is divided into a few categories: positivism, constructivism and interpretivism, among others. Quantitative research is based on positivism, which is an ontological position advocating the existence of only one truth (an objective reality) and is independent of human perceptions (Al-Qeisi, 2009). According to Johnson and Onwuegbuzie (2004), quantitative research focuses on deduction, confirmation of theory or hypothesis testing, prediction and statistical analysis. Meanwhile, qualitative research is based on constructivism and interpretivism (Johnson & Onwuegbuzie, 2004). This paradigm relies on text or image data, which have unique steps in data analysis and draw on diverse strategies of inquiry (Creswell, 2009). On the other hand, mixed-method research is a procedure that combines several research design techniques (quantitative and qualitative, methods, concepts or languages) within a single study to understand a research problem completely (Hesse-Biber, 2010; Johnson & Onwuegbuzie, 2004).

Previous research has reviewed several published mixed-method studies and revealed several purposes in which researchers have used mixed-methods (Venkatesh, Brown & Bala, 2013; Denscombe, 2008) such as:

(i) Mixed-method research has been used by previous researchers to improve the accuracy of the research data.

(ii) Mixed-method research is used to decrease the research bias intrinsic in a single-method approach and to increase the research strengths through a combination of several approaches.

(iii) Mixed-methods have been used as a way of developing the analysis and building on the initial findings using different kinds of data or methods.

Based on the above findings, the current study uses the mixed-method research approach with the purpose of increasing the validity and the strength of the study, and decreasing the research bias. In this study, the quantitative method was used to determine the relationship between the factors in the Health Information System Security Policies Compliance (HISSPC) model and users' compliance behaviour towards Health Information System (HIS) security policies. Meanwhile, the qualitative research was employed to explore the findings from a quantitative research in more depth. The qualitative approach was done during prototype testing. We believe that the combination of several approaches in this study helps in expanding the understanding of the research problem (Hesse-Biber, 2010).

3.3 Justification of the Research Paradigm Chosen

In this study, the priority was given to the quantitative research technique for several reasons. *Firstly,* the vast body of research on human compliance behaviour towards ISPs has applied the quantitative approach (Chang, Wu & Liu, 2012; Herath & Rao, 2009b; Kyobe, 2010; Ng et al., 2009; Warkentin et al., 2011). There is already a significant corpus of literature, known variables and existing theories to support the work undertaken in the current study.

Secondly, the current study adapts the two significant behavioural theories: Theory of Planned Behaviour (TPB) and Health Belief Model (HBM), and the trust factor to develop the HISSPC model. Relevant hypotheses were then developed and tested using Partial Least Squares-Structural Equation Modelling (PLS-SEM) analysis. This study is focused on theory development and prediction, thus, PLS-SEM analysis has been chosen.

In contrast, the qualitative research technique serves as a follow-up to the quantitative study and provides interpretive resources for understanding the results from the quantitative research. This was done during prototype testing. The prototype testing is the stage in which the prototype will be tested by end-users. The HIS prototype was developed based on the significant factors in the HISSPC model that were found during the hypotheses testing (quantitative analysis). The purpose of prototype testing is to further evaluate the HISSPC model in explaining users' compliance behaviour towards HIS security policies through the users' experience of using the proposed system. Qualitative research was used to collect and analyse the interview data during the prototype testing phase. For these reasons, the mixed-method paradigm has been employed in this study.

3.4 Research Design

In this study, the explanatory sequential mixed-method research design was chosen as the research method. Within the explanatory sequential mixed-method research design, one type of data informs the collection of another type of data in a subsequent stage (Creswell, 2009). The sequence of the quantitative and qualitative data collection was determined by the research objectives and research questions. The current study emphasizes the quantitative phase; therefore, previous literatures were reviewed extensively to develop the HISSPC model and research hypotheses. The final questionnaires were distributed to respondents from selected local hospitals and quantitative data were collected through a self-administered survey. The statistical analysis was expected to provide a general understanding of the compliance behaviour issue in the health sector environment by identifying the significant factors concerning users' security compliance behaviour towards ISPs.

In design and development phase, the HIS prototype was designed and developed based on the quantitative survey results using PLS-SEM analysis. Then, the prototype testing was conducted and the data were collected using semi-structured interviews with HIS users. The interviews were conducted at the end of the testing process and the interview data were transcribed and analysed using the qualitative technique to determine the themes; the findings from which were used to support the findings of the quantitative survey results.

The research design in this study contains five phases, which are initial phase, planning phase, quantitative phase, design and development phase as well as qualitative phase, as shown in Figure 3.1.

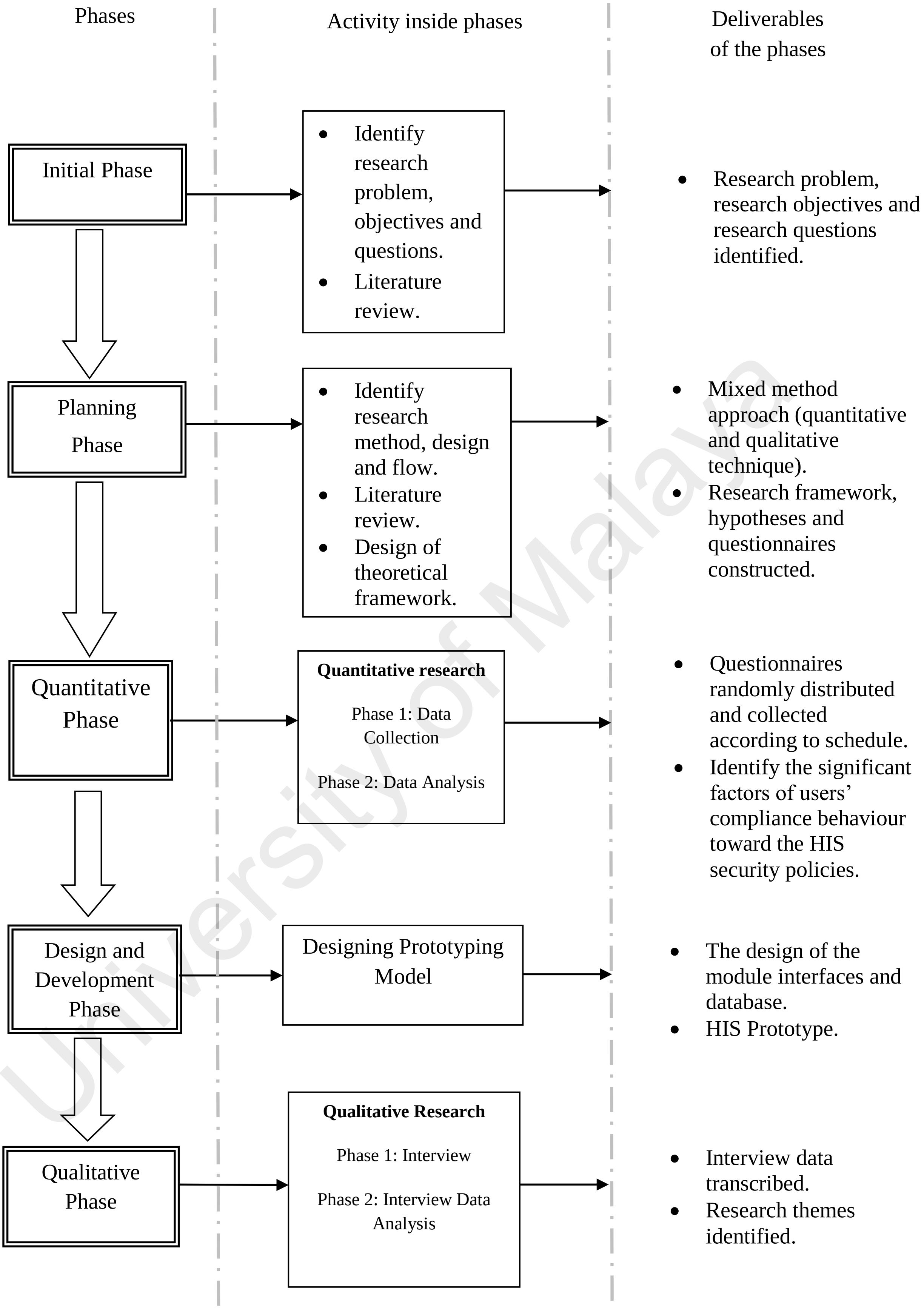

Phases
Activity inside phases
Deliverables of the phases
Initial Phase
Identify research problem, objectives and questions.
Literature review.
Research problem, research objectives and research questions identified.
Planning Phase
Identify research method, design and flow.
Literature review.
Design of theoretical framework.
Mixed method approach (quantitative and qualitative technique).
Research framework, hypotheses and questionnaires constructed.
Quantitative Phase
Quantitative research
Phase 1: Data Collection
Phase 2: Data Analysis
Questionnaires randomly distributed and collected according to schedule.
Identify the significant factors of users' compliance behaviour toward the HIS security policies.
Design and Development Phase
Designing Prototyping Model
The design of the module interfaces and database.
HIS Prototype.
Qualitative Phase
Qualitative Research
Phase 1: Interview
Phase 2: Interview Data Analysis
Interview data transcribed.
Research themes identified.

Figure 3.1: Research Design

3.4.1 Initial Phase

The initial phase revolves around the initial part of the research. In this phase, the research problem was explored and identified. Based on the research problem, the research objectives and research questions were constructed.

3.4.2 Planning Phase

The development of the research model and hypotheses, research process, tool, schedule and budget need to be included in the formal planning process. In this phase, the relevant theories and models were explored and identified to develop the research model through a review of the literature. In doing so, the search strategy to search for articles that are related to the current study is important. The researcher also needs to consider the research method to be chosen in order to accomplish the research objectives and research questions. The current study used the quantitative technique as a principal method and the qualitative technique served as a follow-up to the quantitative study.

3.4.2.1 Search Strategy

The search for related articles was carried out during 2011 and up until 2014. The key terms in the article title, abstract and keyword of the reference article were used in the search strategy, which is information security, information security policies, information security compliance behaviour, and information security effectiveness and information security awareness, etc. In order to reduce the number of empirical articles being searched, a limit was set for articles dated from 2005 until present. This range was chosen because many related studies that are useful in the current study were published during this period. However, concept papers were searched irrespective of the year they were published. The concept paper is a paper that illustrates the outline of the research and discusses why the research is important and how it will be carried out in future.

An extensive literature search was conducted on several electronic databases – ScienceDirect, IEEE Explorer, Emerald, Academic Search Premier @EBSCO host, and SpringerLink. However, most of the reference papers were retrieved from ScienceDirect. Approximately 450 documents were identified through the search process. After reading through the abstract and extensively reviewing the articles, approximately 300 studies that met the inclusion criteria were identified.

3.4.2.2 Inclusion and Exclusion Criteria of Selecting an Article

The following inclusion criteria were used:

(i) The articles must be published in English in a peer-reviewed journal. The articles submitted to peer-reviewed journals were considered as high quality research because these articles have undergone rigorous evaluation. Additionally, these articles were reviewed by a group of subject experts.

(ii) Any empirical research that had been published between 2005 and the present year was selected because it was considered to be relevant to the current study.

(iii) Any concept paper related to information security studies was also included.

The current study adapted human behavioural theories with the aim of investigating factors that influence users' compliance behaviour towards ISPs. Therefore, any technical articles were excluded.

3.4.2.3 Process of Retrieval of References

The process of retrieving the required articles was done in several phases. *Firstly*, titles of the articles were identified and only the titles that matched the research aim and keywords were retrieved. Additionally, only English text papers and those published in peer-reviewed journals were selected for further review.

Secondly, abstracts were read to determine whether the articles complied with the inclusion criteria of the current study. Abstracts that were relevant to the human information security behaviour studies were selected and consequently the full-text articles were retrieved for further review.

Finally, all retrieved full-text articles were thoroughly examined by using content analysis before further review. The selected articles were reviewed in detail to identify any relevant theories to develop a research model for the current study, which will be explained in the following section.

3.4.3 Quantitative Phase

This phase is divided into two parts: (i) data collection and (ii) data analysis. The purpose of this phase is to study the problem in detail. Depending upon the size of the research being undertaken, this phase could be as short as the Preliminary Investigation, or it could take several months.

After the quantitative research survey is done, the data are analysed to identify the significant factors. Then, before the prototype development process starts, the modules of HIS prototype requirements are described in order to ensure that the prototype will perform as expected. The requirement statements should list all of the major details of the programme based on the quantitative analysis that has been done.

3.4.3.1 Data Collection

Before data are collected, a few things need to be decided and planned, as explained below:

a) Population

The population of this study refers to the employees who are working in government hospitals in Malaysia. There are about 134 government hospitals in Malaysia, as listed on the myMalaysia info website. In order to obtain an accurate total of the population, hospitals implementing the Total Health Information System (THIS) were selected. A few government hospitals have implemented THIS in the Klang Valley area. However, only three hospitals gave permission and agreed to participate in this research. These hospitals are Selayang Hospital, Sungai Buloh Hospital and Serdang Hospital, as shown in Table 3.1. Total population for this study was 7760, which is consists of staff from various positions (Doctors, Support Staff and Health Administrator).

Table 3.1: Total of population

Hospitals	**Population**
Selayang Hospital	2937
Sungai Buloh Hospital	2487
Serdang Hospital	2336
Total of Population:	**7760**

b) Sampling Frame

The sampling frame for this study is the health professionals who are the end-users of HIS from various positions, such as nurses, physicians, pharmacists, radiologists, health administrators and doctors. In considering the criteria selection, all of the health professionals who interact with patients or patients’ medical records in the hospital are eligible for selection.

The sampling frame used for this study was obtained from the selected local hospitals. The health professionals were divided into three categories according to their job functions. The three categories of employee identified and named as health professionals are follows:

(i) Doctors

(ii) Support staff, such as the nurses, pharmacists, medical assistants and laboratory assistants

(iii) Health administrators

c) Research Ethics

Prior to conducting the current study, a visit to the hospital was organized, and subsequently, a meeting between the researcher, the hospital management, Clinical Research Centre (CRC) staff and IT staff was conducted. The objective of the meeting was to seek further clarification of the rationale and the status of THIS implementation in these three hospitals. The visit was beneficial, as the information gained was used for planning the logistics for implementing the research tasks and activities.

Moreover, before the data collection begins, a full application for approval was made to the public hospitals, Institute of Health Information System (HIS) and Ministry of Health (MOH). This approval was required to get an approval for data collection. The procedures for the data collection were as follows:

(i) Meeting with the Clinical Research Centre (CRC) officers to get clear instructions on conducting research in the hospitals.

(ii) Registration of the research information in National Medical Research Register System (NMRR).

(iii) Issuance of formal letter on research application to hospitals management.

(iv) After getting all the approval letters from the selected hospitals, researchers upload all the approval letters in NMRR system and submit the application to Institute for Health Systems Research and Ministry of Health (MOH).

(v) Approval of applications is subjected to ethics review.

(vi) Proceed with the data collection.

The current study conducted two stages of data collection: quantitative data and qualitative data. The approval to conduct a quantitative research was given for one year beginning on 19 September 2012 to 19 September 2013. After that, the researcher needed to submit a continuing review form to MOH to apply for another approval for qualitative research. The qualitative research was granted approval for one year from 9 May 2014 until 9 May 2015.

The researcher analysed the data gathered from each individual and treated each respondent as an individual data source. For the interview section, each participant was given a consent letter before the interview was conducted. The purpose of the consent letter was to obtain permission from the participants involved in the interview process, whereby they agree to give full commitment and to inform them that their rights are protected. Details of the participants who are involved in the survey will be protected and kept confidential.

d) Sample Size and Response Rate

Several steps were undertaken to determine the sample size. *Firstly*, the size of the population from the selected government hospitals was identified and calculated to obtain the total size of the population. The list of the population was taken from the Human Resource Department of the respective hospitals. *Secondly*, the strata were divided based on the categories of employee at each selected hospital. *Finally*, the sample size of each stratum was calculated to obtain the final total sample size.

The total population from these three hospitals was 7760 employees. If the population size is more than 5000, an adequate sample size will be 400 to 500 (Singh, Fook, & Sidhu, 2006). However, considering the size of the total population and the amount of error, which in the current study is to be within 5 percentage points (with 95 percent certainty), the sample size calculator was used to determine the required sample size (Krejcie & Morgan, 1970), which in this case was 367.

Formula to calculate the sample size needed for each hospital:

S = (size of hospital population / total of population) * 367 *(1)*

Formula to calculate the sample size needed from each category of employee:

s1 = (total of employee / size of hospital population) * S *(2)*

To avoid any issue of non-response and sampling error, a total of 900 questionnaires were distributed randomly to the respondents. However, only 454 questionnaires were obtained and validated. Another 421 questionnaires were non-responsive and 25 questionnaires were rejected due to missing values. A description of the respondents is presented in Chapter 4.

e) Sampling Technique

In order to choose the sampling technique, the researcher needs to consider the categories of hospital employees, as stated in the previous paragraph. Since the samples of the current study were not homogeneous, stratified random sampling was used to determine the sample sizes, as shown in Table 3.2. Stratified sampling is a procedure used to obtain a greater degree of representativeness while decreasing the probable sampling error (Creswell, 2009). Thus, the stratified sample method was chosen to ensure that an adequate number of respondents were selected from each category of employee at the selected government hospitals.

Table 3.2: Total of sample size from each category of employees

Hospital **Category**	**Selayang Hospital**	**Sungai Buloh Hospital**	**Serdang Hospital**	**Target Total *(s1)***
Health administrators	(266/2937) * 139 = 13	(175/2487) * 118 = 8	(209/2336) * 110 = 10	**31**
Doctors	(699/2937) * 139 = 33	(421/2487) * 118 = 20	(492/2336) * 110 = 23	**76**
Support staff	(1972/2937) * 139 = 93	(1891/2487) * 118 = 90	(1635/2336) * 110 = 77	**260**
Total sample size needed	(2937/7760) * 367 = 139	(2487/7760) * 367 = 118	(2336/7760) * 367 = 110	**367**
Total number of questionnaires distributed	300	300	300	**900**
Total number of responses after validation	159	166	129	**454**
Notes:	*s1* = (total of employee / size of hospital population) * *S* **s1* = minimum total of sample size needed from each category of employees. **S* = minimum total of sample size needed for each hospital			

f) Survey Instrument

The first phase of the current study utilised a survey questionnairewith close ended statements to measure the numerical patterns of demographical profiles, HIS usage and selected subjective constructs using quantitative approach due to its systematic precision of presentation. The survey method has been criticised for its reliance on self-report data (Spector, 1992 as cited by Saidon, 2012). Hair et al. (2003) stated several issues concerning the survey method, such as the difficulty in determining the truthfulness of the answers, the lack of detail and in-depth information, and the lack of control over timeliness. Bearing these issues in mind, the current study adapted a questionnaire that had been previously tested, and was found to be reliable and have a valid scale. However, some of the items in the questionnaire were self-developed. To mitigate any response bias, the survey instrument underwent several validation procedures, such as translation process.

Wellington and Szczerbinski (2007) highlighted several issues that researchers should consider when designing a survey instrument, as stated below:

(i) The questionnaires should be written in a proper sequence. This can help respondents to respond well to each item in the questionnaire.

(ii) Try to avoid questionnaires that are easily misunderstood. If the respondents do not understand the statement written in the questionnaires, it will affect the quality of the data used in this research. Thus, the questionnaires should be simple and easy to read.

(iii) The questionnaires should be written clearly and using simple language. This can help respondents to fully understand the questionnaires and respond effectively. Saidon (2012) suggested that the language used in the questionnaire should be equivalent to the high school level of comprehension.

(iv) Use minimum number of questions. If too many questions or statements are made it would cause respondents to feel bored and too tired to respond to the questionnaire. Then, the quality of the data might be affected. According to Frazer and Lawley (2000), the overall length of the questionnaire should be less than 12 pages, which is the preferred length for a survey.

g) Questionnaire Development and Design

The questionnaire was prepared in two languages – English and Bahasa Melayu (national language). The reason for translating the questionnaire to the Malay language was to ensure that respondents had a solid understanding of the response statement.

The questionnaire was divided into three different sections. Section A captured demographical profiles of health professionals such as age, gender and occupation. Section B presented the perceptions of health professionals on connectivity between human and technical factors (management support, information security awareness, self-efficacy, perceived barriers and perceived trust). Section C evaluated normative thoughts of health professionals on compliance behaviour towards HIS security policies. The identified constructs in Sections B and C were measured using multiple version of adapted items (Table 3.3 – Table 3.8) with 5-point Likert scale (Strongly Disagree, Disagree, Neutral, Agree, strongly Agree) (Likert, 1932).

The total number of items used to measure the independent variables was 44 and four items were used to measure the dependent variable. Overall, there were 48 measurable items. The items used to measure Leadership Behaviour were based on the Leadership Style (transformational leadership and transactional leadership), as stated in Table 3.3. The items were adapted from Aaron (2006) and Bass (1985).

Table 3.3: Items Developed to measure leadership behaviour

Code	Items	Adapted from
Leadership Behaviour		
M06	The leader always encourages me to attend any information security training.	(Aaron, 2006; Bass, 1985)
M01	The leader always seeks for improvements related to information security policies.	
M13	The leader thinks my job performance will improve if I adopt appropriate information security behaviour.	
M03	The leader takes serious action against those who do not comply with information security policies.	
M04	The leader always values the adoption of practicing adequate information security behaviour.	

Management play an important role in preventing information security incidents. This can be done through the implementation of an information security campaign and posters, ISPs training and education programme. The questionnaire developed to measure cues to action and information security policies training and education was adapted from previous studies (Chang et al., 2012; Ng et al., 2009; Meillier et al., 1997). The measurement items are shown in Table 3.4.

Table 3.4: Items developed to measure cues to action and ISPs training and education

Code	Items	Adapted from
Cues to Action		
M11	The management updates me on changes related to information security policies.	(Chang et al., 2012; Ng et al., 2009; Meillier et al., 1997)
M15	Information security articles or newsletters are distributed to all employees in my organization.	
M16	All employees in my organization are always alerted of information security threats through messages/emails.	
M17	All employees in my organization always alerted of any changes related to information security policies through messages/emails/ posters.	
M18	The management organises ongoing information security campaign to increase users' awareness.	
M09	The management documents the information security policies efficiently so that I can understand them easily.	
M10	Information security policies are easy to access in my organization.	
M12	There exists a clear structure for disciplinary action in the case of non-compliance with organization's information security policy.	
M14	Information security policies in my organization help me to understand how to behave appropriately towards matters related to information security.	
Information Security Policies Training and Education		
M02	The management always educates me on the importance of practicing information security policies.	(Chang et al., 2012)
M05	The management always provides specific training on information security regularly.	
M07	The information security training organized by the management is complete.	
M08	The information security training organized by the management is effective.	

In the current study, the items used to measure information security awareness (Perceived susceptibility, Perceived severity and Perceived benefit) were developed based on HBM as well as perceived barrier, as shown in Table 3.5.

Table 3.5: Items developed to measure perceived susceptibility, perceived severity, perceived benefit and perceived barrier

CODE	Items	Adapted from
Perceived Susceptibility		
PSUS19	I am aware that if I do not adopt information security behaviour adequately, it will cause security incidents.	(Ng et al., 2009)
PSUS20	I am aware that if I do not comply with information security policies in my organization, it is a serious problem.	
PSUS21	I am aware that if I do not comply with information security policies, my organization could be subjected to a serious information security threat.	
PSUS24	I am aware that if organizational data are being stolen by an unauthorised user, it is a serious problem.	
Perceived Severity		
PSEV25	I am aware that if I do not follow information security policy the penalty will be severe.	(Siponen et al., 2010; Ng et al., 2009)
PSEV28	I am aware that failure to adopt information security behaviour will jeopardise my career.	
PSEV29	I am aware that failure to adopt information security behaviour will harm my organization’s data.	
Perceived Benefit		
PBEN34	I am aware that using information security countermeasures is effective for reducing security incidents in my organization.	(D'Arcy, Hovav, & Galletta, 2009; Ng et al., 2009)
PBEN35	I am aware that information security countermeasure is effective for protecting my organization’s data.	
PBEN36	I am aware that using a strong password is effective for avoiding unauthorised access.	
PBEN37	I am aware that changing the password regularly is effective for avoiding unauthorised access.	
PBEN38	I am aware that using anti-virus software regularly is effective for protecting my computer.	
PBEN39	I am aware that updating anti-virus software regularly is effective for protecting my computer.	
PBEN40	I am aware that scanning files and devices before using them is effective for protecting my computer.	
Perceived Barrier		
PBAR26	Practicing information security behaviour requires lots of effort such as changing password regularly.	(Ng et al., 2009)
PBAR27	It is difficult to understand my organization’s information security policies.	
PBAR32	Having to learn information security behaviour is a waste of time.	
PBAR33	Adopting information security behaviour is inconvenient.	

The current study believes that trust is an important factor that should be embedded in the organization because it can produce a positive attitude among employees. The trust measurement items developed by Chung and Kwon (2009) were adapted to measure perceived trust, as shown in Table 3.6.

Table 3.6: Items developed to measure trust

CODE	Items	Adapted from
TRUST41	I feel confident of my understanding of the information security policies in my organization.	(Chung & Kwon, 2009)
TRUST42	I feel confident when it comes to implementing information security policies in my organization.	
TRUST43	I feel confident practicing information security policies in my organization.	
TRUST44	I feel confident with the information security policies in my organization.	

On the other hand, the items used to measure self-efficacy were based on TPB (Perceived Behavioural Control). The measurement items were adapted from Ifinedo (2012) and Chan, Woon and Kankanhalli (2005) as shown in Table 3.7.

Table 3.7: Items developed to measure self-efficacy

Code	Items	Adapted from
SE22	I have the necessary skills to recognize many types of information security violations (e.g. Did not change password, suspicious email and did not update anti-virus regularly, etc.).	(Ifinedo, 2012; Chan et al., 2005;)
SE23	I have the necessary skills to protect my organization’s data from information security violations.	
SE30	I have the necessary skills to use information security tools if someone tells me what to do as I go along.	
SE31	I have the necessary skills to implement the available preventive measures to avoid information security threats.	

Finally, the items used to measure health professionals' compliance behaviour towards HIS security policies, which were adapted from Siponen et al. (2010) and Chan et al. (2005) are shown in Table 3.8. HIS security policies compliance behaviour is a dependent variable in the current study.

Table 3.8: Items developed to measure the dependent variable

CODE	**Items**	**Adapted from**
UCB45	I comply with information security policies when performing my daily work.	(Siponen et al., 2010; Chan et al., 2005)
UCB46	I practice the recommended information security behaviour as much as possible.	
UCB47	I always recommend others to comply with information security policies.	
UCB48	I assist others in complying with information security policies.	

h) Validity and Reliability of the Instrument

The instrument used in the current study was tested for validity and reliability to ensure a high quality measure. In order to check the validity of questionnaires, content validity was chosen in order to measure how well the items represent the entire universe of items. This process underwent several stages, as discussed below.

All of the measurement items adapted in this study were written in English and have been tested previously, mostly in Western countries. Since this study was conducted in Malaysia and the sample of this study consisted of non-English speakers, the questionnaire needed to go through the *translation process* in an attempt to minimise any possible variance due to cultural and linguistic differences (Kim and Han, 2004 as cited by Saidon, 2012).

Brislin et al. (1973, as cited by Saidon, 2012) suggested one or more of the following translation techniques, i.e. back-translation, bilingual techniques, committee approach and pre-test. Back translation refers to the process in which the target language version is translated back into the source language version. Meanwhile, the bilingual technique refers to the testing process of both the source and target language versions among bilingual respondents in order to detect any discrepancies in the two versions. On the other hand, the committee approach involves a team of bilingual people to translate from the source to the target language. Finally, a pilot study was carried out in the pre-test procedures after the completion of the translation process with the aim to ensure that the future respondents of the target language version could understand the questionnaires completely.

Among these techniques, back-translation is highly recommended in the previous literature, and the most widely used in cross-cultural research (Shaw & Erickson, 2014; Saidon, 2012; Brislin, 1970). In doing so, two bilingual translators competent in both English and Malay were involved in the translation process. The first translator translated from the source language (English) into the target language (Malay). Another translator who was not familiar with the measurements used in the questionnaire served as the back translator. At this time, the Malay version was then translated back into the English version. Once completed, the questionnaire with dual languages (English and Malay) was reviewed by two experts in the field of study before the questionnaires were distributed to the respondents.

A *pilot study* was conducted in early 2012 in which the questionnaire was randomly distributed to 42 respondents, who were then excluded from the actual respondents in the population. The pilot study was conducted to make sure that the respondents understood the items in the questionnaire and to ensure that there was no confusion in the questions that would lead to ambiguity. In doing this, a discussion was carried out with some of the pilot-study respondents in order to refine the questionnaire. Other pilot-study respondents were also asked to write a comment at the end of the questionnaire.

One issue that was raised during the discussion with the pilot-study respondents was the length of the questionnaire. The pilot group felt that it was too long and contained some vocabulary that participants may not understand. The current study considered this issue when refining the final questionnaire. In doing so, the questionnaires items were checked thoroughly and any redundant items will be removed. Moreover, this study also hired an expert to check the vocabulary used in the questionnaires.

The reliability of the pilot-study questionnaire was assessed based on the Cronbach's alpha coefficient. According to Hair et al. (2010), the lower acceptance limit of Cronbach's alpha is 0.60 to 0.70. In this research, the range of reliability results for each construct in the pilot study was from .713 to .917, as shown in Table 3.9; all within the acceptable range described in the literature.

Table 3.9: Pilot study reliability analysis

Constructs	Cronbach's alpha coefficient (α)
Independent	
Management Support	
Leadership behaviour:	
• Transformational leadership	.800
• Transactional leadership	.865
ISPs Training and Implementation	.905
Information Security Awareness	
Perceived benefit	.825
Perceived severity	.810
Perceived susceptibility	.858
Others:	
Perceived barriers	.713
Self-efficacy	.838
Perceived trust	.917
Dependent	
Users' compliance behaviour	.872

After the pilot study was completed successfully, the final questionnaires (Appendix A.1) were distributed to the respondents of the sample in the larger population as hard copies and hand delivered by the researcher. The distribution of the final questionnaires was carried out in December 2012 and the data collection was completed within six months.

3.4.3.2 Data Analysis

The current study employed the Statistical Package for Social Sciences (SPSS) version 21.0 to analyse the data in the first phase. The SPSS was used to screen the data in terms of coding and normality. Skewness and kurtosis were used to analyse the normality of the data.

Additionally, to gain an overview of the data, SPSS was also used to apply exploratory factor analysis (EFA). The data concerning the demographic background of the respondents were analysed for frequency and percentage. In addition, SPSS was also used to perform the non-response (if necessary) and common method bias tests.

Then, in the second phase of data analysis, Structural Equation Modelling (SEM) analysis was applied using Smart Partial Least Squares (SmartPLS) version 2.0 (Ringle, Wende, & Will, 2005) to test the measurement model and structural model of this study. Essentially, there are two approaches to run SEM analysis – the covariance-based approach and PLS approach. Various software can be used to test the covariance-based approach, such as Analysis of Moment Structures (AMOS), Linear Structural Relationship (LISREL), and Structural Equation Modelling Software (EQS). Meanwhile, PLS analysis can be found in software, such as SmartPLS, PLS-Graph, Latent Variable PLS (LVPLS), among others. However, PLS-SEM was chosen in this study because it is a useful and flexible tool for statistical building.

SmartPLS is a variance-based software, which is suitable for causal predictive analysis, especially in the condition of high complexity and low theoretical information (Barclay, Higgins, & Thompson, 1995). Meanwhile, AMOS-SEM or LISREL-SEM is covariance based, which is best used for theory testing and development (Hair, Ringle, & Sarstedt, 2011). PLS-SEM allows the measurement model (relationships between constructs and indicators) and structural model (theoretical relationships among constructs) to be tested simultaneously, with an adequate PLS measurement model, the hypotheses could be tested by examining the PLS structural model. The explanatory power of the PLS structural model was assessed based on the amount of variance in the endogenous constructs in the research model. Moreover, PLS-SEM does not impose multivariate homogeneity or the normality requirement on the data (Kankanhalli et al., 2003).

SEM methodology is claimed to be useful in the behavioural and social sciences in which many constructs are unobservable (Sharma, 1996). SEM helps researchers to assess the unidimensionality, reliability and validity of each construct in the research model. Recently, SEM has become a common statistical tool applied in academic research (Hair, et al., 2010). Moreover, the literature confirms that SEM is the outstanding method of multivariate data analysis (Chin & Dibbern, 2010). Applying SEM to test the hypothesized relationships between factors allows a complete investigation of all the hypothesized relationships simultaneously including the relationships among the multiple dependent variables in a study (Hair et al., 2011).

The premise of the current study is more about predictive analysis whereby the conceptual model of the study can be categorised as prediction-oriented modelling. For that reason, PLS-SEM was applied to test the hypotheses.

Figure 3.2 illustrates the flow of data analysis procedures applied in this study. The data analysis consists of two phases: preliminary analysis and PLS-SEM analysis.

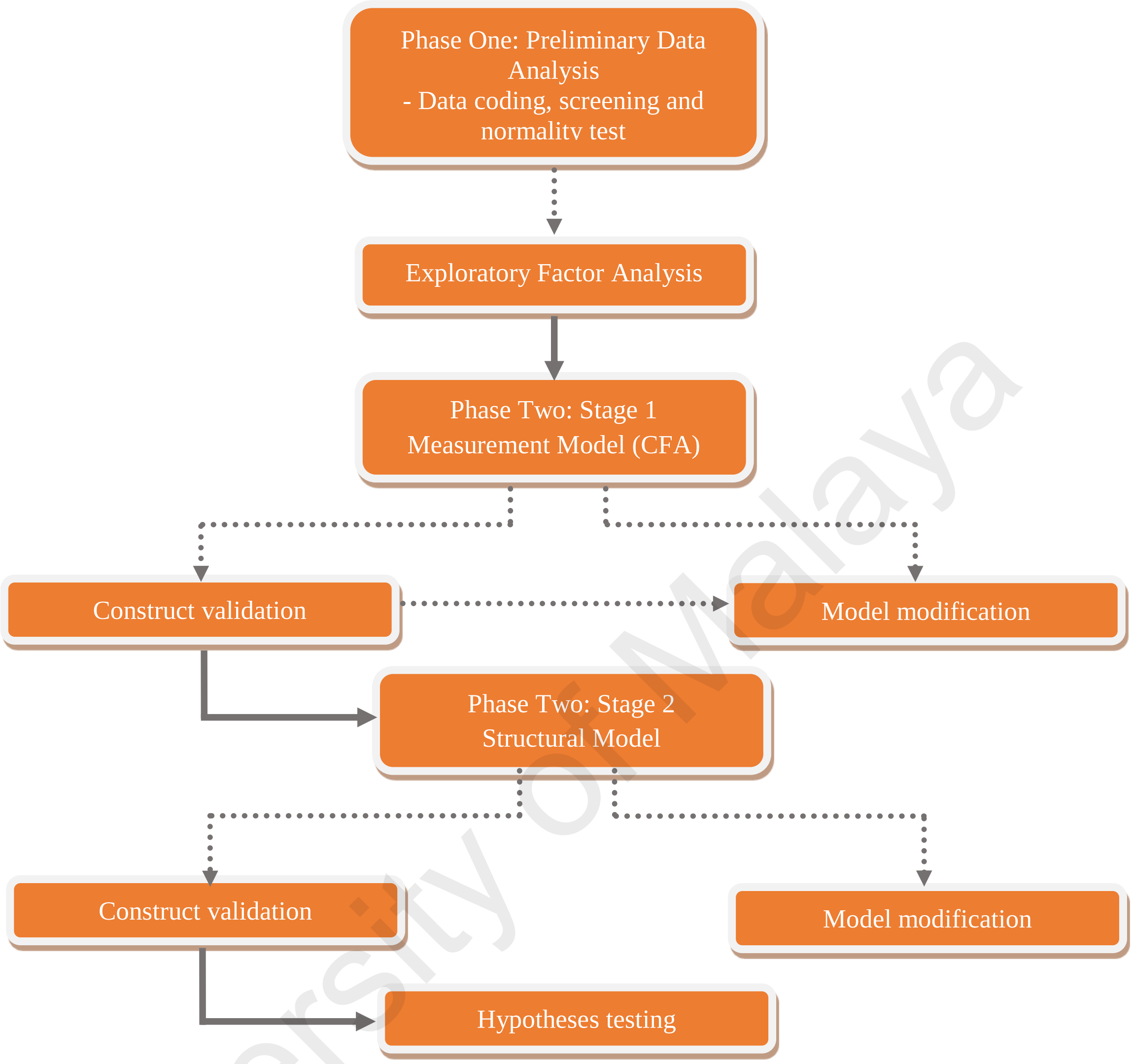


Figure 3.2: Flow of data analysis

The first phase of data analysis deals with the data screening procedures in order to ensure that the data have been correctly entered, and to test the normality of the data. After data coding, the screening and normality test were successfully conducted, EFA was carried out to identify how many factors could be retained by exploring the loadings value of the items used to measure each construct and to try to achieve the best model before the research model was tested in the second phase of the research.

The second phase was the application of a two-stage PLS-SEM process. Stage one was to assess the measurement properties of PLS-SEM, which involved the assessment of the unidimensionality of each latent variable, model re-specification or modification and the test of reliability and the validity of the measurement properties. The second stage involved specification of the paths relationship between the underlying theoretical latent constructs. If all the measurements are valid, the structural model can be used for hypotheses testing. PLS-SEM analysis was applied using SmartPLS 2.0 to determine the significant predictor and to achieve research objective two (RO2). The details are explained in Table 3.10.

Table 3.10: Quantitative data analysis plan

Research Objectives	**Research Questions/Concepts**	**Measurement**	**Scale**	**Analysis/ Statistic**
RO1: To develop Health Information System's Security Policies Compliance (HISSPC) model.	RQ1: What are the factors used to develop HISSPC model?	Research framework development		Literature Review Exploratory factor analysis (EFA) Descriptive analysis
RO2: To determine the relationships between the factors in the HISSPC Model and users' compliance behaviour towards Health Information System (HIS) security policies.	RQ2: What is the relationship between the factors in the HISSPC model and users' compliance behaviour towards HIS security policies? Sub-questions: RQ2.1: To what extent does the indicated factor in the HISSPC model influence users' compliance behaviour towards HIS security policies?	Questionnaires	Likert scale (1-5) (1) Strongly agree (2) Agree (3) Neutral (4) Disagree (5) Strongly disagree	PLS-SEM analysis Multi-group analysis

Research Objectives	Research Questions/Concepts	Measurement	Scale	Analysis/ Statistic
	RQ2.2: To what extent does the intervening factor in the HISSPC model influence users' compliance behaviour towards HIS security policies? RQ2.3: To what extent does the HIS usage experience moderate the influence of the factors in the HISSPC model on users' compliance behaviour towards HIS security policies?			

a) Factor Analysis: Exploratory Factor Analysis and Confirmatory Factor Analysis

When the study has many constructs and indicators, the research model is considered complicated (Hair et al., 2011). Therefore, to reduce the complexity of the research model, EFA was conducted to identify how many factors can be retained by exploring the loading values of the items used to measure each construct and to achieve the best model before the research model was tested using PLS (Preacher and MacCallum, 2002). Furthermore, EFA was conducted because some of the relationships among the observed indicators and underlying factors were neither tested nor investigated beforehand.

EFA was applied in the final study to achieve research objective one (RO1). Principal component analysis with orthogonal varimax rotation was chosen to identify the underlying factors based on the following steps: (i) The extraction of the initial factors; (ii) The rotation to a terminal solution; and (iii) The selection of the number of factors.

In addition, confirmatory factor analysis (CFA) was conducted to test how well the final instrument measured the particular constructs in the research model. This was done through convergent and discriminant validity. Furthermore, Cronbach's alpha was used for the purpose of the measurement of reliability for numerical data and its purpose was to determine how well the items positively correlate to one and another.

b) Justifications for Using PLS-SEM

The most appropriate SEM approach should be selected based on the researcher's objectives (Christmas, 2005). The goal of this study is to predict or identify the significant factors of HIS security policies compliance behaviour. Therefore, PLS-SEM was chosen because PLS-SEM is an exploratory methodology that relies on the data and it is used to obtain determinate values for latent variables for predictive purposes and minimise the variance of all dependent variables.

Other advantages that can be found in PLS-SEM over the covariance-based approach are that PLS-SEM is able to handle complex models and is insensitive to data size. The research model is considered complex when it has a large number of variables and indicators (Hair et al., 2010), such as the research model adapted in this study.

c) Reliability Test in PLS-SEM

Reliability is important because it can minimise the errors and biases in research (Hair et al., 2010). In PLS-SEM analysis, there are two types of reliability test that need consideration: indicator reliability and construct reliability. Indicator reliability is used to specify which part of an indicator's variance can be explained by the underlying latent variable while construct reliability is used to assess how well a construct is measured by its assigned indicators (Götz, Liehr-Gobbers & Krafft, 2010). The reliability of the indicators can be assessed by checking their factor loading (λ) values, whereby, as suggested by many authors of previous studies, values larger than 0.7 are acceptable (Chin, 1998; Götz et al., 2010; Hair et al., 2010). This study employs two methods to assess the reliability of the constructs in the research model: (i) Cronbach's alpha and (ii) composite reliability (CR).

Cronbach's alpha is the most common method used to assess construct reliability (Sekaran, 2003). In fact, it has been considered as the first method one should use to assess the reliability of a measurement scale (Lorence & Churchill, 2005). Different levels of acceptance have been suggested in the literature. For instance, Hair et al. (2011) suggested that the alpha value should exceed 0.70 to indicate internal consistency. On the other hand, Carmines and Zeller (1979) suggested a level of acceptance of 0.80 for internal consistency. As for new scales, a level of 0.60 is considered acceptable (Hair et al., 2010; Nunnally & Bernstein, 1994). Despite the various views on the level of acceptance, it is generally agreed that an alpha of 0.70 and over is acceptable to indicate internal consistency. Therefore, this study uses 0.70 as the minimum level to indicate the internal consistency of the constructs.

Other construct reliability tests that are also important include composite reliability (CR). This is important to ensure that all the measures used in this study are reliable, and at the same time, provide greater confidence to the researcher that the individual items are consistent in their measurements (Hair, Ringle & Sarstedt, 2013). CR is used to check how well a construct is measured by its assigned indicators (Götz et al., 2010). The authors of previous studies related to security policies compliance behaviour also suggested that the acceptable recommended value for CR is equal to or greater than 0.60 (Herath & Rao, 2009b).

d) Validity Test in PLS-SEM

Validity is defined as *"the degree to which a measure accurately represents what it is supposed to"* (Hair et al., 2010, p. 7). Two types of validity, namely, content validity and construct validity (convergent and discriminant validity) are measured in this study.

Content validity is the assessment of the extent the content of a scale measures a construct (Hair et al., 2010).In order to obtain content validity, careful attention was given to the process of developing the questionnaires. In this study, the researcher constructed the measurement items based on previous literature and modified some of the measurement items to suit the study. Further, the questionnaires went through a back translation process. During this process, the comments and suggestions from experts (practitioners in health institutions and academician experts) regarding the wording of the items in the questionnaires were obtained. Any ambiguous words or sentences were corrected. The process of questionnaire validation has been explained in a previous section.

On the other hand, construct validity is the extent to which a set of measured items actually reflects the latent construct the items are designed to measure (Hair et al., 2010). Construct validity is examined by analysing both convergent and discriminant validity. According to Sekaran (2003), the convergent validity examines whether the measures of the same construct are highly correlated, whereas discriminant validity determines whether the measures of a construct are too highly correlated with other constructs in the research model.

To establish convergent validity, Average Variance Extracted (AVE) was used. AVE includes indicators variance which is captured by the construct relative to the total amount of variance, including the variance due to measurement error (Götz et al., 2010). The threshold value of AVE suggested by previous studies is 0.50 or higher, otherwise it is considered insufficient (Hair et al., 2013; Götz et al., 2010). On the other hand, discriminant validity is established when the estimated correlations between the constructs do not exceed 0.85 (Awang, 2012; Kline, 2005). Hulland (1999, as cited by Götz et al., 2010) stated that the shared variance between a construct and its indicators should be larger than the shared variance with other constructs, so that the discriminant validity will be achieved. As this study used PLS to conduct SEM analysis, the test of goodness-of-fit is not necessary.

e) Multi-Group Analysis

Multi-group PLS analysis approach was used to test the moderator effect of duration of using HIS among health professionals. The HIS experience among health professionals was measured using an item asking “In general, how long are you working with HIS?” The median value for this measure was 2.0 on a 4-point scale ranging from “less than 1 year” to “more than 10 years”. Based on the median result, the current study categorises the health professionals who have experience using HIS for more than five years under the high experience group. Meanwhile, health professionals who have lower experience using HIS (less than 5 years) were categorised under the low experience group. This is in line with previous researchers who argued that employees who have less than five years of working experience are considered as inexperienced employees (Bulgurcu et al., 2009; Kanai-Pak, Aiken, Sloane, & Poghosyan, 2008).

To test the moderating effect of HIS experience among health professionals, this study follows the test proposes by Venkatesh & Morris (2000), whereby, the models in PLS were separated into three groups: Full Model, High model and Low Model. The differences of all three models were tested using test for differences suggested by Chin (2016). The analysis was further explained in Chapter 4.

3.4.4 Design and Prototype Development Phase

The design phase was divided into two parts: logical design and detailed design. The logical design consisted of activities, such as designing the system database using Unified Modelling Language (UML) through which the Use Case view and logical view of the HIS prototype was developed. On the other hand, the detailed design consisted of activities, such as designing users interface and developing the system database. HIS is an interactive website, so it requires a server-side scripting language that can interact with a database server. Hence, the PHP language was chosen to develop the HIS prototype and MySQL was chosen to develop the system database for several reasons, as stated in the following (Bates, 2006; MySQL, 2014):

(i) PHP is a powerful scripting language for creating dynamic and interactive websites.

(ii) MySQL provides amazing performance results and offers a high reliability of database server system.

(iii) Both PHP and MySQL are open source software and free to download and use.

(iv) Both PHP and MySQL are platform independent, i.e. they can be run under Windows, Linux and Unix.

(v) Both PHP and MySQL are easy to use.

3.4.4.1 Prototype Development Methodology

The HIS prototype was developed to manage HIS security policies announcements or notifications for all employees in health institutions effectively and systematically. Several design stages were performed in the development of each HIS module based on the Waterfall Model. In the Waterfall Model, the system development process cascades from one phase to another (Ali & Aydah, 2012). The design stages included in this study were the Partial Least Squares-Structural Equation Modeling (PLS-SEM) analysis, the identification of users, determining the system requirements, the interaction between objects used in the design, and, finally, the prototype implementation and testing, as shown in Figure 3.3.

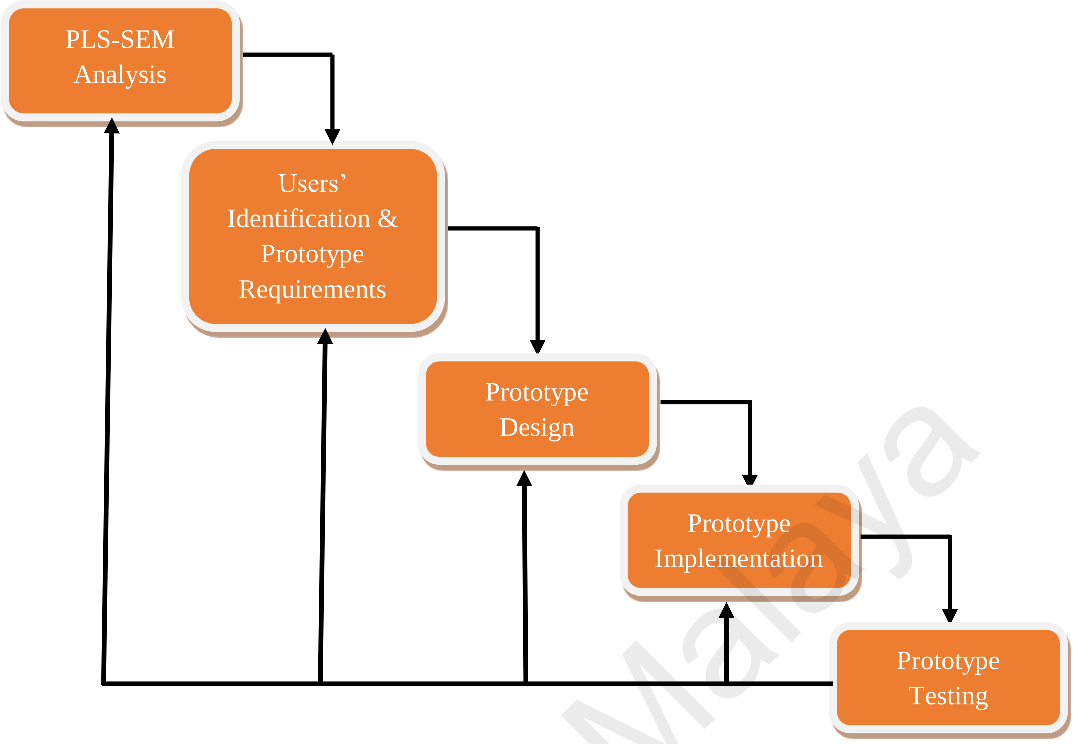


Figure 3.3: Prototype Development Life Cycle (PDLC)

The first stage of the PDLC for the HIS prototype development was the PLS-SEM analysis, in which the significant factors that influenced health professionals' information security compliance behaviour were identified. Then, based on the PLS-SEM analysis results, the prototype requirements were described in the second stage according to each category of the user. The interaction between the objects used in the design was described using the Unified Modeling Languages (UML), through which the researcher's model used the case view and logical view of the prototype before the prototype module interfaces were designed. This was carried out in the third stage of the PDLC. The fourth stage of the PDLC was the implementation of the prototype, in which the prototype was developed and installed. Finally, the prototype was tested by the HIS users and the recommended module of the HIS prototype was evaluated. The evaluation was based on the Health Information System Security Policies Compliance (HISSPC) model.

3.4.5 Qualitative Phase

This phase is also divided into two parts: (i) data collection and (ii) data analysis. The purpose of this phase is to explore user's compliance behaviour towards HIS in detail through user's experience using the prototype. The qualitative results would help to support the results found in quantitative findings.

3.4.5.1 Data Collection

Since most of qualitative data are non-numeric, the ways to gather these data collection largely emphasize the "realism" of investigated subjects. Qualitative data collection technique range from interviews, observational techniques such as participation observation and fieldwork, through to archival research. In this study, qualitative data collection was done during prototype testing. The prototype testing was conducted to determine whether the prototype modules were effective to improve users' compliance behaviour towards ISPs by analysing users' experience with the proposed system. The prototype reflects the partial application of HIS concentrated on the HISSPC model. The findings of the prototype testing provide an empirical evaluation for the prototype created.

The data collection began by selecting typical sample as a method to choose the participants that were involved in this study. For this reason, the main participants that were involved included the health professionals responsible in keeping and managing patient's health records using HIS such as doctors, pharmacist and nurses. These health professionals were believed to have wide knowledge and experience on the process of managing health records using HIS. This study also interviewed several health administrators who handled health records. The types of sampling method that has been adopted for qualitative research in this study was snowball sampling. The snowball sampling is *"a strategy involves the locating of a few key participants that easily meet the criteria that we have established for participating in the study"* (Merriam, 2009, pg. 70).

The sample size involved in this study depended on the information that would be collected because the sample size was based on the information that would be considered. This argument illustrates that the sample size is determined. Merriam (2009) has also highlighted that the sample size is determined by a number of factors relevant to the purpose of the study. In this study, the sample size involved was determined throughout the process of data analysis. For this reasons, 18 participants were involved in this study.

a) Interviews

Once the prototype was developed, it was then tested by health professionals who were the end-users of HIS. Then, interviews were conducted once the users completed the testing process. Interviews were chosen as they were able to provide depth to a particular issue. The interviews were recorded on audio tapes and transcribed after the interviews ended.

The interview questions were semi-structured and allowed open-ended responses. However, the open-ended responses were controlled to ensure that the interview topics were covered and did not go beyond the research scope. Through these interviews, information was collected pertaining to users perception towards complying with health information system security policies and their perceptions towards the current module of the HIS prototype that might help to improve compliant behaviours towards ISPs. The semi-structured interviews were guided by open-ended questions that served as a data collection guide. The open-ended questions were self-developed as shown in Appendix A.2.

Each participant was given a consent letter before the interview was conducted. The purpose of consent letter was to obtain permission from the participants involved in the interview process, whereby they agreed to give full commitment and to inform them that their rights were protected. The details of the participants who were involved in the interview would be protected and kept confidential.

3.4.5.2 Qualitative Data Analysis

A qualitative data analysis of the data obtained during the interviews after prototype testing was used as a follow-up complementary method and provided interpretative resources, insights and an explanation of the study (Creswell, 2009; Watson, Cosio, & Lin, 2014). In this study, we used the thematic analysis approach to analyse the interview data to achieve research objective three (RO3), as shown in Table 3.11. The thematic analysis is a foundational method in qualitative analysis to search for themes or patterns from interview data (Braun & Victoria, 2006). The qualitative data analysis tool used in this study was ATLAS.ti version 7.1 to analyse and organise interview data.

Table 3.11: Qualitative data analysis plan

Research Objective	**Research Question**	**Measurement**	**Scale**	**Analysis**
RO3: To evaluate the HISSPC model using a Health Information System (HIS) prototype.	RQ3: How can the prototype be used to improve users' compliance behaviour towards HIS security policies?	Interviews	Open-ended questions	ATLAS.ti 7.1 • Thematic analysis

a) Steps in Thematic Analysis

To ensure that the interview data were analysed in a proper way, this study followed Braun and Victoria's thematic analysis guideline. The six-steps in thematic analysis introduced by Braun and Victoria (2006) are as follows:

(i) Transcribe interview data into written form and familiarise it through reading. The reading should be done multiple times because it helps to identify the patterns before the coding starts.

(ii) Search for potential themes by assessing and organising the data items.

(iii) Generate potential coding ideas. The coding can be generated as many times as relevant.

(iv) Combine and refine the themes based on their separate generations.

(v) Finalise the themes and sub-themes to generate thematic maps. The thematic maps were used to depict a visual representation of the interview data. At this time, the researcher validated the emergent themes and the accuracy of the thematic maps was also evaluated.

b) Data Coding Procedure

The data coding is the process by which categories of responses are established for open-ended questions (Merriam, 2009). It seems that coding is a separation of statement in the process of interpreting new materials. According to Boijie (2010), coding is the process of *"categorizing data segments with a short name that simultaneously summarizes and accounts for each piece of data"* (pg. 95). It is also mentioned that coding involves the analysing of material beyond a concrete statement in the data. The researcher needs to distinguish themes and name them by code attribute. The code attribute was based on several concepts that are revealed from quantitative results.

This study has adopted several coding processes with the aim to establish a concept that results from qualitative findings. Corbin and Strauss (2014) stated that there are three types of coding, namely open coding, axial coding and selective coding. The open coding is a process of *"which concepts are identified and their properties and dimensions are discovered in a data"* (Corbin & Strauss, 2014, pg. 101). The data that are collected are read very carefully and divided into fragments, which are then compared and grouped according to category that deal with the same subject. This category is labelled with a code, which is usually used during the first stage of the coding process.

The second type of coding is known as axial coding and is referred to as a *"set of procedures whereby data are put back together in new ways after open coding by making connections between categories"* (Corbin & Strauss, 2014, pg. 96). This coding is a more abstract process and consists of coding around several single categories or axes. The axial coding is also called focus coding because the coding is based on categories and moves to subcategories, and it is more specific (Charmaz, 2006). The main purpose of axial coding is to determine which elements in the research are the dominant ones and which are not. The second purpose of axial coding is to reduce and recognise the data set.

The last type of coding that has been adopted in this study is known as selective coding. This type of coding looks for connections between the categories in order to make sense of what is happening in the case. The aim of this coding is to integrate the loose piece of the earlier coding.

c) Reliability and Validity of Interview Data

The reliability of qualitative data was substantiated by using triangulation method of comparing data from interviews and quantitative findings. The discussions on reliability have been debated by scholars such as Creswell (2012), Yin (2009) and Merriam (2009). These authors have their views on the use of triangulation method as a strategy in ensuring the reliability of the information. As reminded from their works, triangulation means comparing the data by using documentation or comparing the data gathered from other method. Furthermore, triangulation is also used to validate interview data (Merriam, 2009).

Inter-rater reliability technique also was employed in this study, whereby, other analyst was hired to analyse the interview data. This technique can help to improve the consistency or reliability of data analyses.

d) Qualitative Data Analysis Software - Atlas.Ti

Atlas.Ti was used to analyse interview data, which means to identify the codes and themes. Atlas.Ti handles and keeps track of all data and they are saved in a container called hermeneutic unit or HU. Atlas.Ti HU can be understood as a container which holds everything that needs to be interpreted such as quotes, code, words notes, memos links, code families and super codes (Susanne, 2012).

CHAPTER 4: QUANTITATIVE ANALYSIS, RESULTS & DISCUSSION

4.1 Introduction

This chapter explains the analysis conducted and presents the empirical results to test the research hypotheses. This chapter consists of six main sections. It starts with an introduction and follows with the preliminary analysis of the data, which describes the procedures undertaken to purify the data in the second section. The second section also provides an explanation of the evaluation of the response rate, including the non-response bias test and a general description of the survey respondents.

Furthermore, the second section also reports the exploratory factor analysis (EFA) results followed by the results of the Common Method Bias (CMB) testing. The results of Confirmatory Factor Analysis (CFA) that was used to test the measurement model are presented in section three, which covers the assessment of unidimensionality, reliability and construct validity. Meanwhile, the results of the structural model to test the hypotheses developed in the Chapter Two, are reported in section four. The predictive relevance and power analysis of the research model also presented in section four. Section five discusses the results of the multi-group analysis. Finally, discussion of the research findings concludes this chapter in section six.

4.2 Preliminary Data Analysis

Preliminary data analysis is essential to ensure that the quantitative data used in this study are error-free and can proceed with Partial Least Square-Structural Equation Modelling (PLS-SEM) analysis. The preliminary analysis included data editing and coding, data screening and data normality. In this phase, exploratory factor analysis (EFA), descriptive analysis and common method biases test were also carried out.

4.2.1 Data Editing and Coding

After completing the data collection process, editing of the raw data was carried out to ensure the completeness of the data. Editing involved checking the data collection forms for omissions, legibility and consistency in classification (Pallant, 2007).

Then, the raw data were manually entered into a data file in Statistical Package for Social Sciences (SPSS) version 21.0. There are two major ways to exercise this process: pre-coding or post-coding (De Vaus, 1995). This study applied the pre-coding method whereby all the measurement items were pre-coded with numerical values. Any out of range values were revisited and corrected where appropriate.

4.2.2 Data Screening

Data screening was done to ensure that the data were correctly entered and to confirm that the distribution of variables was normal. Skewness and kurtosis were measured to test the normality of data. The value of skewness and kurtosis for each item was in the range of -1.96 to +1.96 as shown in Appendix B. This result indicated that the data were normally distributed. However, all observations were retained for analysis as this study used PLS-SEM, for which data normality is not a requirement to pursue further analysis.

4.2.3 Response Rate

In order to get higher rate of respondents, 300 questionnaires were distributed to each selected hospital (Hospital Selayang, Hospital Sungai Buloh and Hospital Serdang). However, only 479 out of 900 questionnaires were returned, which is equivalent to a 53.2 per cent response rate. Another 421 questionnaires were classified as non-response and after data checking, only 454 questionnaires (50.4%) were validated and another 25 questionnaires (2.8%) were rejected due to missing values. The summary on the rate of return of the questionnaire is illustrated in Table 4.1.

Table 4.1: Summary on the rate of return of questionnaires

	Number of questionnaires	**Percentage/Reasons**
Total questionnaires distributed	900 (300 * 3 hospitals)	100%
Questionnaires returned	479	53.2%
Unusable questionnaires	25	2.8% questionnaires were rejected due to serious missing values
Usable questionnaires	454	50.4%

The response rate in this study was considered appropriate based on the following reasons. *Firstly*, the researcher managed to collect more data than the target of the sample sizes required for this study (n = 367) based on the calculation of the sample size explained in Chapter Three.

Secondly, the rate of 50.4 per cent was based on the total of questionnaires distributed, but not based on the actual sample size required. Thus, this study considered that the actual response rate was 100 per cent.

Finally, the response rate of 50.4 per cent is still acceptable since in many previous studies the response rate is within the common range of 12 to 60 per cent (Al-Omari et al., 2013; Brady, 2011; Herath & Rao, 2009b; Ng et al., 2009). Moreover, due to several difficulties in data collection in this sensitive context, a response rate of more than 19% is considered reasonable (Uffen & Breitner, 2013). Therefore, for these given reasons, the researcher concluded that the non-response bias is not an issue in this study.

4.2.4 Profile of Respondents

The overall demographic results show that there were more females, with 357 respondents (78.6%), than males, with 97 respondents (21.4%). The majority of the respondents were aged between 20 and 40 years (n = 394, 86.7%) and the rest were more than 40 years old (n = 60, 13.2%). Approximately 50.2 per cent of the respondents (n = 228) had less than 5 years of HIS usage in the hospital while the remaining 49.8 per cent of the respondents (n = 226) had more than 5 years of HIS experience.

Most of the respondents were support staff (nurses, pharmacists, radiologists, medical assistants, etc.) with a total of 278 respondents (61.3%), followed by doctors (n = 132, 29%) and health administrators (n = 44, 9.7%). The majority of the respondents were from Sungai Buloh Hospital (n = 166, 36.6%), followed by Selayang Hospital (n = 159, 35%) and Serdang Hospital (n = 129, 28.4%).

Moreover, for HIS experience group, the total number of respondents for the high experience users was 226 while for the low experience users was 228. The summary of demographical profiles for each group is presented in Table 4.2.

Table 4.2: Demographical profiles of health professionals in selected Malaysian hospitals

	HIS usage					
	Full **n = 454**		**High Experience** **n = 226**		**Low Experience** **n = 228**	
Demographics	**Frequency**	**Percentage (%)**	**Frequency**	**Percentage (%)**	**Frequency**	**Percentage (%)**
Gender						
Male	97	21.40	54	23.90	43	18.90
Female	357	78.60	172	76.10	185	81.10
Age						
< 40 years	394	86.70	167	77.50	227	99.50
>= 40 years	60	13.20	59	22.50	1	0.50
Hospital						
Selayang	159	35.00	88	38.90	71	31.10
Sungai Buloh	166	36.60	78	34.50	88	69.70
Serdang	129	28.40	60	26.50	69	30.30
Position/Occupation						
Doctors	132	29	63	27.9%	69	30.30
Support staffs	278	61.30	136	58.00	142	62.40
Health administrators	44	9.70	27	11.90	17	7.40

4.2.5 Exploratory Factor Analysis (EFA)

To answer RQ1, the Exploratory Factor Analysis (EFA) was conducted to identify how many factors can be retained by exploring the loadings value of items used to measure each construct before the research model being tested using PLS.

The EFA was conducted in several stages. *Firstly*, the suitability of the data for factor analysis was assessed, whereby all 44 items used to measure the independent variables and another four items used to measure the dependent variables were tested separately. The results revealed that the Kaiser-Meyer-Olkin (KMO value) was less than 0.6 for the independent variables, which means that the value was not appropriate for factor analysis (Pallant, 2007). Therefore, some of the items used to measure the independent variables needed to be deleted. In doing so, the communality values indicating the amount of variance in each item were examined. Communality values of less than 0.5 indicate that an item does not fit well with the other items in its component (Pallant, 2007), and, hence, can be removed so that the scale can be improved to increase the total variance explained.

Secondly, the factor loading for each item was also examined and factor loading values of less than 0.4 were removed (Hair et al., 2010; Pallant, 2007).

Finally, three items for the independent variables were removed, as shown in Table 4.3. Thus, the final EFA was conducted with 41 items used to measure the independent variables.

Table 4.3: Item removed from independent variables

Construct	**Measurement Item**	**Reasons**
Management support: Information security policies training and education	MS02: The management always educates me on the importance of practicing information security policies.	Low value of factor loading (0.493)
Perceived benefit	PBEN34: I am aware that using information security countermeasure is effective for reducing security incidents in my organization.	Low value of factor loading (0.484)
Perceived barrier	PBAR26: Practicing information security behaviour requires lots of effort such as changing password regularly.	Loaded separately than other indicated construct.

The KMO of the sampling adequacy for 41 items used to measure the independent variables was 0.929 and the Bartlett’s test of Sphericity value was significant (i.e. a significant value should be p = .05 or smaller). The Chi-Square value was 13653.542, suggesting that the data matrix had sufficient correlation to the factor analysis. The results show that factor analysis can be carried out for further analysis. Using principal component analysis (PCA) with Varimax rotation, the seven constructs (Management Support, Perceived Severity, Perceived Benefit, Perceived Susceptibility, Self-Efficacy, Perceived Barrier and Trust) were retained, which explained approximately 68% of the total variance (eigenvalues greater than 1). This study used PCA instead of principal axis factoring because the aim of PCA is to reduce the number of variables by creating linear combinations that retain as much of the original measures’ variance as possible (without interpretation in terms of constructs) (Pett, Lackey & Sullivan, 2003).

The EFA results showed that all the indicators used to measure leadership behaviour, cues to action and ISPs training and education loaded into one factor. This factor was name as Management Support, while other indicators loaded into the constructs that represent the indicators. These seven constructs were used in Confirmatory Factor Analysis (CFA).

Meanwhile, the KMO for the four items used to the measure dependent variable was 0.716 and the overall significance of the correlation matrix was p = 0.000 with a Bartlett’s test of Sphericity. The Chi-Square value was 1125.248. Only one factor was yielded and explained 73% of the variance in the data with eigenvalues greater than 1. Thus, this result indicated that the four items used to measure the dependent variable should be retained.

Table 4.4 illustrates the final rotated factor as well as the statistical data relating to each factor.

Table 4.4: Factor loadings for independent variables and dependent variable based on a principle components analysis with Varimax rotation.

Factor	**No of items**	**Eigenvalues**	**% of Variance**
Independent Variables			
Management Support	17 items	14.46	35.27
Perceived Benefit	6 items	4.50	10.98
Trust	4 items	2.55	6.21
Perceived Susceptibility	4 items	1.86	4.54
Self-Efficacy	4 items	1.84	4.50
Perceived Severity	3 items	1.51	3.68
Perceived Barrier	3 items	1.14	2.78
		Cumulative % of Variance Values:	67.68%
		KMO	0.929
		Bartlett test of Sphericity	p = 0.000
Dependent Variables			
HIS security policies compliance behaviour	4 items	2.91	72.77%
		KMO	0.716
		Bartlett test of Sphericity	p = 0.000

The HISSPC Model and research hypotheses under management support were modified based on the EFA results, as shown in Figure 4.1 and Table 4.5.

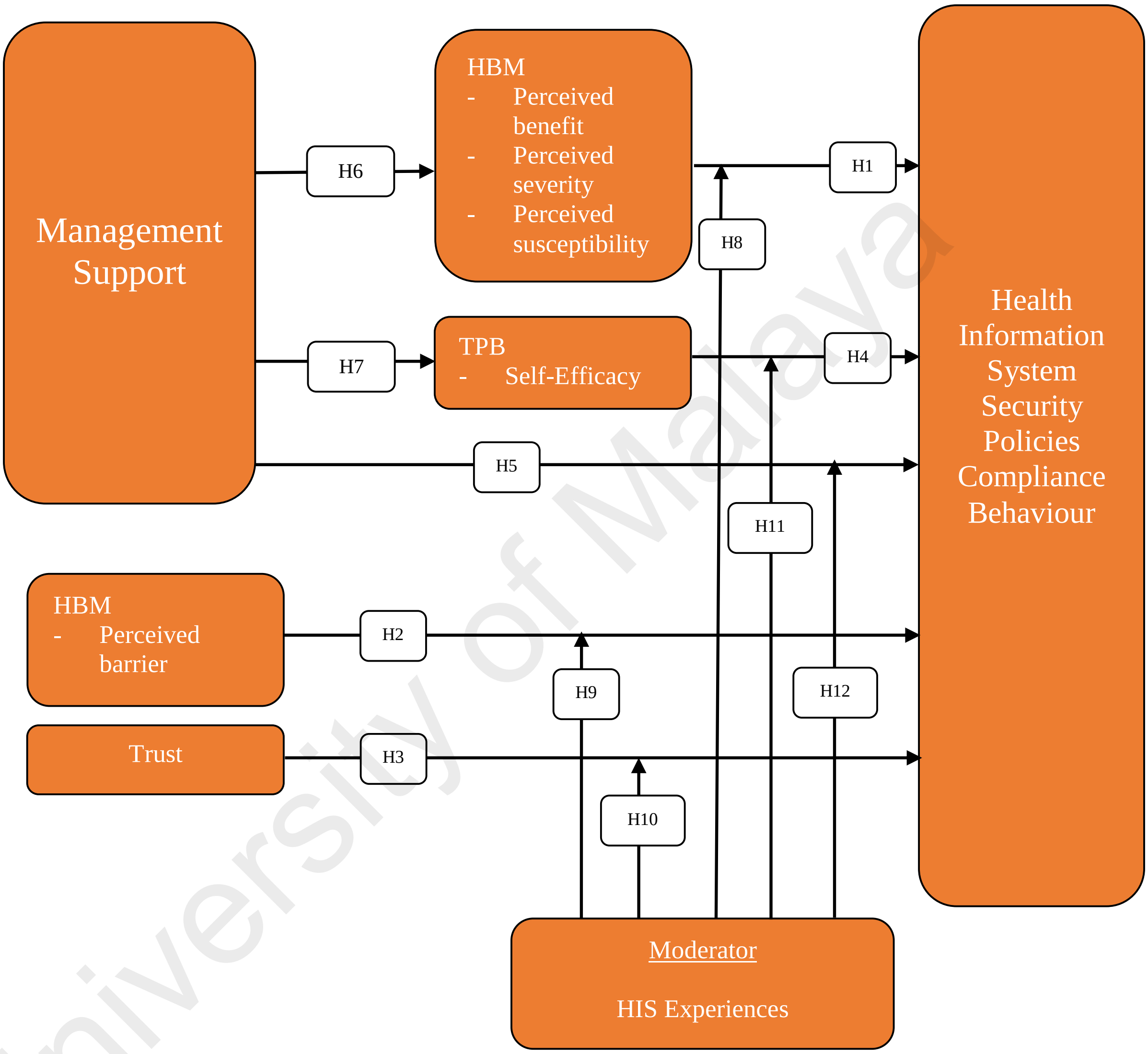


Figure 4.1: Modified HISSPC Model

Table 4.5: Research hypotheses for Management Support construct

Previous Research Hypotheses	Modified Research Hypotheses
H5(a)*: Leadership behaviour will have a positive effect on HIS security policies compliance behaviour.* ***H5(b)****: Cues to action will have a positive effect on HIS security policies compliance behaviour.* ***H5(c)****: Information security policies training and education will have a positive effect on HIS security policies compliance behaviour.*	***H5:*** *Management support will have a positive effect on HIS security policies compliance behaviour.*
H6(a-i)*: Leadership behaviour will have a positive effect on perceived benefit.* ***H6(a-ii)****: Leadership behaviour will have a positive effect on perceived severity.* ***H6(a-iii)****: Leadership behaviour will have an effect on perceived susceptibility.* ***H6(b-i)****: Cues to action will have a positive effect on perceived benefit.* ***H6(b-ii)****: Cues to action will have a positive effect on perceived severity.* ***H6(b-iii)****: Cues to action will have a positive effect on perceived susceptibility.* ***H6(c-i)****: Information security policies training and education will have a positive effect on perceived benefit.* ***H6(c-ii)****: Information security policies training and education will have a positive effect on perceived severity.* ***H6(c-iii)****: Information security policies training and education will have a positive effect on perceived susceptibility.*	***H6(a):*** *Management support will have a positive effect on perceived benefit.* ***H6(b)****: Management support will have a positive effect on perceived severity.* ***H6(c)****: Management support will have a positive effect on perceived susceptibility.*
H6(d-i)*: Leadership behaviour will have a positive indirect effect on HIS security policies compliance behavior through perceived benefit.* ***H6(d-ii)****: Leadership behaviour will have a positive indirect effect on HIS security policies compliance behavior through perceived severity.* ***H6(d-iii)****: Leadership behaviour will have a positive indirect effect on HIS security policies compliance behavior through perceived susceptibility.*	***H6(d)****: Management support will have a positive indirect effect on HIS security policies compliance behavior through perceived benefit.* ***H6(e)****: Management support will have a positive indirect effect on HIS security policies compliance behavior through perceived severity.* ***H6(f*** *Management support will have a positive indirect effect on HIS security policies compliance behavior through perceived susceptibility.*

Previous Research Hypotheses	Modified Research Hypotheses
H6(e-i)*: Cues to action will have a positive indirect effect on HIS security policies compliance behavior through perceived benefit.* ***H6(e-ii)****: Cues to action will have a positive indirect effect on HIS security policies compliance behavior through perceived severity.* ***H6(e-iii)****: Cues to action will have a positive indirect effect on HIS security policies compliance behavior through perceived susceptibility.* ***H6(f-i)****: Information security policies training and education will have a positive indirect effect on HIS security policies compliance behavior through perceived benefit.* ***H6(f-ii)****: Information security policies training and education will have a positive indirect effect on HIS security policies compliance behavior through perceived severity.* ***H6(f-iii)****: Information security policies training and education will have a positive indirect effect on HIS security policies compliance behavior through perceived susceptibility.*	
H7(a)*: Leadership behaviour will have a positive effect on self-efficacy.* ***H7(b)****: Cues to action will have a positive effect on self-efficacy.* ***H7(c)****: Information security policies training and education will have a positive effect on self-efficacy.* ***H7(d)****: Leadership behaviour will have a positive indirect effect on HIS security policies compliance behaviour through self-efficacy.* ***H7(e)****: Cues to action will have a positive indirect effect on HIS security policies compliance behaviour through self-efficacy.* ***H7(f)****: Information security policies training and education will have a positive indirect effect on HIS security policies compliance behaviour through self-efficacy.*	***H7(a)****: Management support will have a positive effect on self-efficacy.* ***H7(b)****: Management support will have a positive indirect effect on HIS security policies compliance behaviour through self-efficacy.*
H12(a)*: Low experience users significantly moderate the positive relationship between leadership behaviour and compliance behaviour towards HIS security.*	***H12****: Low experience users significantly moderate the positive relationship between management support and compliance behaviour towards HIS security policies.*

Previous Research Hypotheses	Modified Research Hypotheses
H12(b)*: Low experience users significantly moderate the positive relationship between cues to action and compliance behaviour towards HIS security policies.* ***H12(c)****: Low experience users significantly moderate the positive relationship between information security policies training and education, and compliance behaviour towards HIS security policies.*	

4.2.6 Common Method Bias (CMB)

In recent decades, many empirical studies have devoted considerable attention to the concept of common method variance (CMV) and how it may bias the results of empirical analyses that use respondents as data sources (Jakobsen & Jensen, 2015). Therefore, before proceeding with CFA, Harman's single-factor test was conducted to assess the Common Method Bias (CMB). CMB is defined as "variance that is attributable to the measurement method rather than to the constructs the measure represent" (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003, p. 289), which could be problematic.

The basic assumption of Harman's single-factor test is that if a substantial amount of CMV is present, a factor analysis of all the data will result in a single factor accounting for the majority of the covariance in the variables. An unrotated single-factor analysis of all study items explained less than 50% per cent of the variance, as shown in Table 4.6. Given that a single factor solution did not emerge and a general factor did not account for most of the variance, CMB was not viewed as a significant threat in this current study (Podsakoff & Organ, 1986a).

Table 4.6: Common method bias testing

Total Variance Explained						
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	18.702	35.287	35.287	18.702	**35.287**	**35.287**
2	5.568	10.506	45.793			
3	2.730	5.150	50.943			
4	2.176	4.106	55.049			
5	1.931	3.644	58.693			
6	1.625	3.066	61.759			
7	1.268	2.393	64.152			
8	1.243	2.345	66.498			
9	1.130	2.132	68.630			
10	1.011	1.908	70.538			

4.3 Confirmatory Factor Analysis (CFA): Measurement Model - Stage One

The first step in PLS-SEM analysis is to analyse the measurement model (outer model) to determine how well the indicators load on the constructs. The measurement model was developed and tested before proceeding with structural model testing. The purpose of measurement model was to measure how the observed variables depend on the unobserved variables or latent variable (Hair et al., 2010). This will ensuring that the survey instrument is reliable. The measurement model was assessed separately for the full model and each model of the groups for multi-group analysis. For this purpose, CFA was administered.

The CFA was conducted to test how well the developed instrument measures particular constructs in the research model. This was done by examining the reliability and validity of the construct. *Firstly*, we looked at the respective loadings in bold and cross loadings from Table 4.7 to assess if there were problems with any particular variable indicators in the full model. Cross loadings were computed to determine if the items loaded on other constructs equally as well as on their respective construct. The current study used a cut-off value of 0.7 or higher for loadings to be considered significant (Hair et al., 2010). The results (Table 4.7) show that most of the indicators measuring a particular construct had loading values of more than 0.7 on their respective constructs except items code PBAR27 (0.667) and MS07 (0.673). The factor loading of items code BAR2 and MS07 are nearly to 0.7; thus, the items are still acceptable. The results confirmed that the indicators were valid for their respective constructs.

Table 4.7: Factor loadings and cross loadings

Constructs /Items	**PBAR**	**PBEN**	**MS**	**SE**	**PSEV**	**PSUS**	**PTRUST**	**UCB**
PBAR27	**0.667**	-0.012	-0.095	0.130	-0.058	-0.010	0.001	-0.077
PBAR32	**0.789**	-0.088	0.085	0.260	-0.035	0.002	-0.091	-0.071
PBAR33	**0.915**	-0.087	0.021	0.153	-0.113	-0.091	-0.163	-0.133
PBEN35	-0.149	**0.743**	0.348	0.251	0.497	0.497	0.518	0.556
PBEN36	-0.123	**0.834**	0.327	0.215	0.485	0.446	0.480	0.551
PBEN37	-0.029	**0.786**	0.277	0.318	0.418	0.417	0.388	0.408
PBEN38	-0.029	**0.843**	0.285	0.231	0.378	0.400	0.370	0.445
PBEN39	-0.046	**0.861**	0.294	0.204	0.385	0.402	0.408	0.473
PBEN40	0.015	**0.788**	0.263	0.296	0.364	0.328	0.419	0.419
MS01	-0.009	0.352	**0.768**	0.311	0.323	0.319	0.386	0.427
MS03	0.021	0.264	**0.717**	0.324	0.429	0.371	0.398	0.373
MS04	-0.072	0.348	**0.767**	0.348	0.394	0.396	0.469	0.483
MS05	0.037	0.215	**0.782**	0.333	0.278	0.294	0.393	0.401
MS06	-0.037	0.199	**0.731**	0.330	0.233	0.231	0.402	0.393
MS07	0.005	0.169	**0.673**	0.242	0.231	0.152	0.419	0.298
MS08	-0.003	0.181	**0.773**	0.293	0.241	0.201	0.395	0.321
MS09	-0.021	0.265	**0.757**	0.351	0.264	0.270	0.494	0.406
MS10	0.029	0.274	**0.781**	0.359	0.365	0.307	0.375	0.402
MS11	0.009	0.301	**0.797**	0.395	0.329	0.321	0.421	0.400
MS12	0.024	0.280	**0.786**	0.358	0.430	0.349	0.375	0.369
MS13	0.034	0.332	**0.759**	0.499	0.401	0.356	0.393	0.405
MS14	-0.065	0.402	**0.820**	0.443	0.408	0.389	0.491	0.446
MS15	-0.026	0.177	**0.755**	0.358	0.237	0.187	0.390	0.401
MS16	0.066	0.339	**0.778**	0.377	0.331	0.341	0.362	0.417
MS17	0.030	0.305	**0.803**	0.388	0.334	0.330	0.332	0.380

Constructs								
/Items	PBAR	PBEN	MS	SE	PSEV	PSUS	PTRUST	UCB
MS18	0.057	0.305	**0.798**	0.432	0.325	0.330	0.372	0.440
SE22	0.129	0.313	0.370	**0.810**	0.271	0.308	0.238	0.311
SE23	0.193	0.249	0.471	**0.812**	0.263	0.260	0.294	0.330
SE30	0.197	0.218	0.265	**0.771**	0.343	0.169	0.315	0.345
SE31	0.168	0.214	0.403	**0.819**	0.272	0.193	0.331	0.349
PSEV25	-0.054	0.463	0.458	0.275	**0.811**	0.581	0.424	0.446
PSEV28	-0.070	0.417	0.365	0.345	**0.879**	0.434	0.476	0.478
PSEV29	-0.129	0.455	0.257	0.267	**0.837**	0.474	0.406	0.417
PSUS19	0.006	0.404	0.353	0.273	0.470	**0.848**	0.383	0.339
PSUS20	0.004	0.363	0.374	0.253	0.463	**0.873**	0.401	0.362
PSUS21	0.000	0.465	0.351	0.237	0.554	**0.856**	0.390	0.416
PSUS24	-0.193	0.503	0.289	0.217	0.496	**0.774**	0.398	0.450
TRUST41	-0.033	0.526	0.474	0.352	0.489	0.410	**0.840**	0.577
TRUST42	-0.086	0.406	0.441	0.284	0.453	0.390	**0.883**	0.597
TRUST43	-0.143	0.527	0.463	0.327	0.491	0.453	**0.919**	0.685
TRUST44	-0.158	0.442	0.478	0.332	0.402	0.402	**0.886**	0.636
UCB45	-0.145	0.556	0.440	0.338	0.464	0.409	0.663	**0.840**
UCB46	-0.109	0.565	0.424	0.339	0.539	0.460	0.632	**0.871**
UCB47	-0.064	0.443	0.465	0.355	0.432	0.381	0.542	**0.843**
UCB48	-0.100	0.453	0.458	0.386	0.369	0.341	0.563	**0.855**

Legends: MS – Management Support; PBAR – Perceived Barrier; PBEN – Perceived Benefit; PSEV – Perceived Severity; PSUS – Perceived Susceptibility; PTRUST – Perceived Trust; SE – Self-Efficacy; UCB – HIS security policies compliance behaviour.

Next, as suggested by Hair et al. (2010), the Composite Reliability (CR) and Average Variance Extracted (AVE) was examined to assess the convergence validity of the measurement items for the full model as shown in Table 4.8. In the full model, the CR for each construct ranged from 0.837 to 0.964, which exceeded the recommended value of 0.7 (Hair et al., 2010). Meanwhile, the AVE for each construct in the full model ranged between 0.590 and 0.727, which is greater than 0.5; thus, the cut-off values ensure that at least 50% or more of the variances in the construct were explained by the set of indicators. The collected data were verified for reliability by calculating the Cronbach’s Alpha (CA). The resulting values ranged from 0.713 to 0.957, which are acceptable. The results of the measurement in the full model show that all seven constructs are valid measures based on their parameter estimates and statistical significance.

Then, we proceeded to test the discriminant validity by examining the squared correlations between the measures of potentially overlapping constructs for full model. The results showed that all diagonal values in bold were higher than the values in the row and column, indicating adequate discriminant validity. This means that no overlapping construct existed. The collected data were also verified for their reliability by calculating the CA. The resulting values in the full model (Table 4.8) ranged from 0.713 to 0.957. The CA results were acceptable because they all exceeded 0.7 (Hair et al., 2013). Table 4.9 show the summary of an assessment of reflective measurement model for full model.

Table 4.8: Convergent and reliability validity

Full Model

				Correlation of constructs							
Models/Constructs	Cronbach's α	Composite Reliability	AVE	MS	PBAR	PBEN	PSEV	PSUS	TRUST	SE	UCB
Full Model											
MS	0.957	0.961	0.590	**0.768**							
PBAR	0.713	0.837	0.635	0.006	**0.797**						
PBEN	0.895	0.920	0.656	0.372	-0.082	**0.810**					
PSEV	0.797	0.880	0.711	0.435	-0.096	0.528	**0.843**				
PSUS	0.858	0.904	0.703	0.406	-0.056	0.519	0.593	**0.839**			
TRUST	0.905	0.934	0.779	0.525	-0.122	0.539	0.519	0.469	**0.882**		
SE	0.817	0.879	0.645	0.478	0.213	0.309	0.353	0.291	0.366	**0.803**	
UCB	0.875	0.914	0.727	0.523	-0.125	0.596	0.533	0.469	0.708	0.415	**0.852**

Note: Diagonal elements in the ‘correlation of constructs’ matrix are the square root of average variance extracted (AVE). For adequate discriminant validity, diagonal should be greater than corresponding off-diagonal elements.

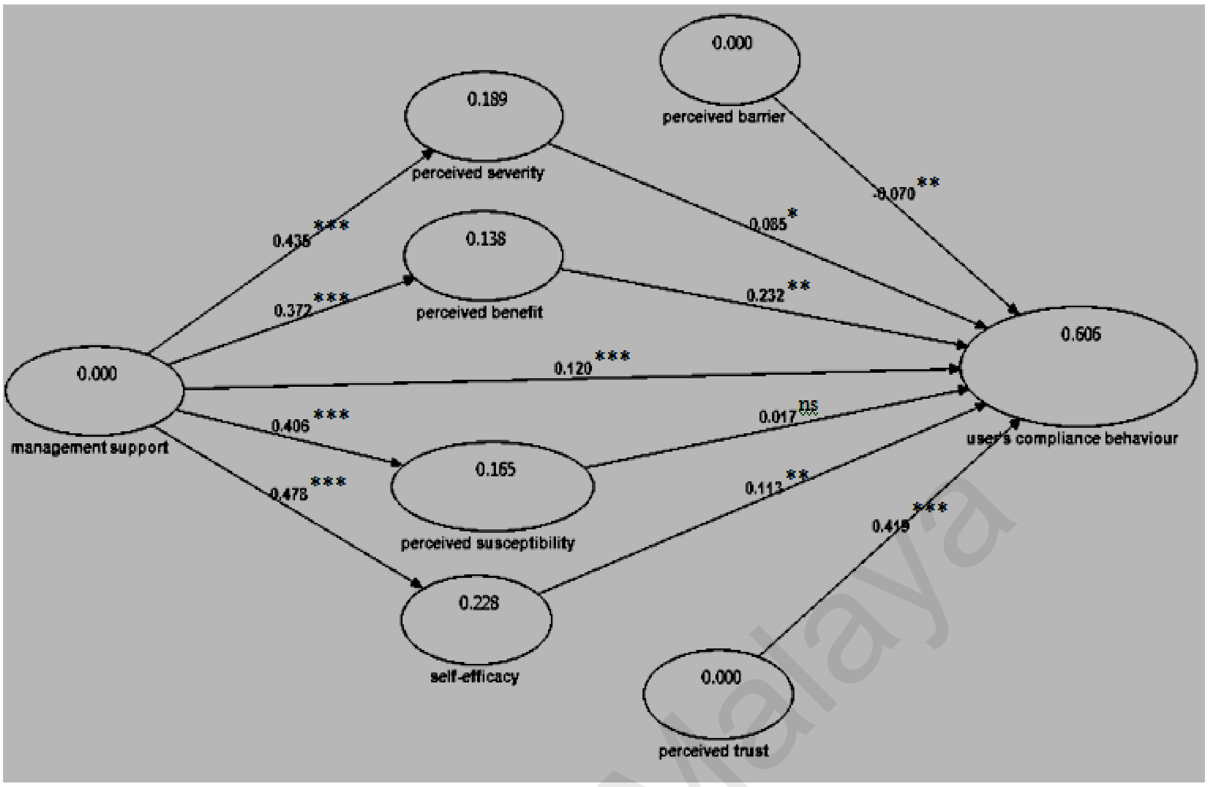
Legends: MS – Management Support; PBAR – Perceived Barrier; PBEN – Perceived Benefit; PSEV – Perceived Severity; PSUS – Perceived Susceptibility; TRUST – Trust; SE – Self-Efficacy; UCB – HIS security policies compliance behaviour.

4.4 Structural Model: Stage Two

Composite reliabilities, discriminant and convergent validities as stated in Table 4.8, have fulfilled the adequacy of psychometric properties within the designed structural model. Bootstrapping with 500 re-samples was used to calculate the path estimate and robust t-statistics for the hypothesized relationships. PLS-SEM does not assume that the data is normally distributed, which implies that parametric significance tests (e.g., as used in regression analyses) cannot be applied to test whether coefficients such as outer weights, outer loadings and path coefficients are significant. Instead, PLS-SEM relies on a nonparametric bootstrap procedure (Davison and Hinkley, 1997; Efron and Tibshirani, 1986) to test the significance of estimated path coefficients in PLS-SEM. The findings are discussed in the next section.

4.4.1 Hypotheses Testing – Direct Effect

In Figure 4.2, the PLS results in the full sample group model were tested without suggesting a moderating effect of HIS experience. The results showed (Figure 4.2) that 18.9 per cent of variance for Perceived Severity, 16.5 per cent of variance for Perceived Susceptibility, 13.8 per cent of variance for Perceived Benefit and 22.8 per cent of variance for Self-Efficacy were explained by Management Support. Meanwhile, 60.6% of variance for compliance behaviour of HIS security policies was explained by Perceived Severity, Perceived Susceptibility, Perceived Benefit, Perceived Barrier, Trust and Self-Efficacy.



Note: *p < 0.1, **p < 0.05, ***p < 0.01, ns – not significant

Figure 4.2: Full Model

The research hypotheses presented in the previous chapter are tested in a statistically significant way. The hypotheses testing showed the positive direct effect of Self-Efficacy (β = 0.113**), Perceived Severity (β = 0.085*), Perceived Benefit (β = 0.232***) and Trust (β = 0.415***) on users' compliance behaviour of ISPs related to HIS policies were significant, while Perceived Susceptibility was not significant (β = 0.017). Meanwhile, Perceived Barrier was found negatively direct effect (β = -0.070**) on users' compliance behaviour of ISPs. Overall, it was found that Trust was the most significant predictor of HIS security policies compliance behaviour. These results provide support *for H1(a), H1(b), H2, H3* and *H4* whereas *H1(c)* was rejected.

On the other hand, Management Support was found to have a positive significant influence on Self-Efficacy (β = 0.478***), HIS security policies compliance behaviour (β = 0.120***), Perceived Severity (β = 0.435***), Perceived Susceptibility (β =

0.406***) and Perceived Benefit of security-countermeasure (*β* = 0.372***). Thus, *H5, H6(a)* until *H6(c),* and *H7(a)* were accepted. The overall hypotheses testing are shown in Table 4.09.

Table 4.09: Direct effect of hypotheses testing

Hypotheses	**Relationships**	**Beta**	**SE**	**t-values**	**Decision**
H1(a)	Perceived Benefit -> HIS security policies compliance behaviour	0.232	0.043	*5.385****	*Accepted*
H1(b)	Perceived Severity -> HIS security policies compliance behaviour	0.085	0.051	*1.656**	*Accepted*
H1(c)	Perceived Susceptibility -> User's compliance behaviour	0.017	0.054	0.312	Rejected
H2	Perceived Barrier -> HIS security policies compliance behaviour	-0.070	0.033	*2.141***	*Accepted*
H3	Trust -> HIS security policies compliance behaviour	0.415	0.039	*10.807****	*Accepted*
H4	Self-Efficacy -> HIS security policies compliance behaviour	0.113	0.045	*2.533***	*Accepted*
H5	Management Support ->HIS security policies compliance behaviour	0.120	0.039	*3.086****	*Accepted*
H6(a)	Management Support -> Perceived Benefit	0.372	0.037	*10.163****	*Accepted*
H6(b)	Management Support -> Perceived Severity	0.435	0.044	*9.925****	*Accepted*
H6(c)	Management Support -> Perceived susceptibility	0.406	0.047	*8.697****	*Accepted*
H7(a)	Management Support -> Self-Efficacy	0.478	0.044	*10.890****	*Accepted*

Note: Significance value of two tailed (Hair et al., 2011): *p < 0.1, t =>1.645; **p < 0.05, t >= 1.96; ***p < 0.01, t => 2.58

4.4.2 Mediation Effect of Information Security Awareness and Self-Efficacy

The research model posited four mediators (Perceived Benefit, Perceived Severity, Perceived Susceptibility and Self-Efficacy). In this regard, this study applied Preacher and Hayes (2004, 2008) mediation testing procedure, whereby the new method called bootstrapping of the indirect effect was used. Bootstrapping, a non-parametric resampling procedure has been recognized as one of the more rigorous and powerful methods for testing the mediating effect (Zhao, Lynch & Chen, 2010; Hayes, 2009). The application of bootstrapping for mediation analysis has recently been advocated by Hair et al. (2013) who noted that "when testing mediating effects, researchers should rather follow Preacher and Hayes (2004, 2008) and bootstrap the sampling distribution of the indirect effect, which works for simple and multiple mediator models" (p. 223).

Furthermore, the bootstrapping method is said to be perfectly suited for PLS-SEM because it makes no assumption about the shape of the variables' distribution or the sampling distribution of the statistic (Hair et al., 2013).

The bootstrapping was run to get the t-value to assess if the direct relationship are significant before testing the mediating effects. The criteria for mediation analysis must adequately meet up as follows: first, the predictor (Management Support) has significant influence on the mediators (Perceived Benefit, Perceived Severity, Perceived Susceptibility and Self-Efficacy); second, the mediators have significant influence on the dependent variable (User's Compliance Behaviour); third, the predictor (Management Support) has significant influence on the dependent variable (User's Compliance Behaviour) in the absence of the mediators' influence (Perceived Benefit, Perceived Severity, Perceived Susceptibility and Self-Efficacy). Now, to establish the mediating effect, the bootstrapping with a resample of 500 was used and that produced 500 bootstrapped direct effect. Then, to test the indirect effect of the indicated constructs, the researcher needs to do manually in Excel to get the t-value. In this regard, the z statistic suggested by Sobel (1982, as cited by Akter et al., 2011a), which is significant at p < 0.05. If the t value exceeds 1.96 (p < 0.05), then, the indirect effect was accepted. However, the t value exceeds 1.65 (p < 0.1) is still acceptable (Hair et al., 2011).

The bootstrapping analysis showed that Perceived Severity (*β* = 0.043*) and Perceived Benefit (*β* = 0.087***) were positive significant in the relationship between Management Support and compliance behaviour of security policies related to HIS. Management Support has no indirect effect through the extent of Perceived Susceptibility (*β* = 0.012). Thus, *H6(d)* and *H6(e)* were accepted while *H6(f)* was rejected.

The results also show that Management Support has an indirect effect with HIS security policies compliance behaviour through the extent of Self-Efficacy (*β* = 0.479***). Therefore, *H7(b)* was accepted. The indirect effect of hypotheses testing is presented in Table 4.10.

Table 4.10: Indirect effect of hypotheses testing

Hypotheses	**Relationships**	**Beta**	**SE**	**t-values**	**Decision**
H6(d)	Management Support -> Perceived Benefit ->HIS security policies compliance behaviour	0.087	0.019	*4.590****	*Accepted*
H6(e)	Management Support -> Perceived Severity ->HIS security policies compliance behaviour	0.043	0.023	*1.872**	*Accepted*
H6(f)	Management Support -> Perceived Susceptibility ->HIS security policies compliance behaviour	0.012	0.022	0.556	Rejected
H7(b)	Management Support -> Self-Efficacy ->HIS security policies compliance behaviour	0.479	0.042	*11.285****	*Accepted*

Note: Significance value of two tailed (Hair et al., 2011): *p < 0.1, t >= 1.65; **p < 0.05, t >= 1.96; ***p < 0.01, t => 2.58

4.4.3 Predictive Relevance (PR), Effect Size and Power Analysis of Full Model

The predictive relevance of the research model was tested using the blindfolding technique. Based on blindfolding procedure, Q^2 evaluates the predictive validity of a large complex model using PLS. While estimating parameters for a model under blindfolding procedure, this technique omits data for a given block of indicators and then predicts the omitted part based on the calculated parameters. Thus, Q^2 shows how well the data collected empirically can be reconstructed with the help of model and the PLS parameters (Akter, D'Ambra, & Ray, 2011b).

According to the results, as shown in Table 4.12, using an omission distance (D) of 7, this study obtains a Q^2 of 0.44, which is more than the cut-off value 0.0 (Hair et al., 2011, 2013), thereby indicating that the research model in this study has predictive relevance. The relative impact of the research model calculated by obtaining q^2 showed that Perceived Severity and Perceived Susceptibility have no relative impact while others with values of more than 0.0, but lower than 0.15, indicated a small impact. In addition, this study used the Stone-Geisser approach to assess whether a predictor variable has a substantive influence on the endogenous construct by exploring the effect size of f^2. Chin (1998, p. 317) stated that the higher the f^2, the greater the influence of the exogenous construct whereby values of 0.02, 0.15 and 0.35 can be respectively regarded as small, medium or large effect respectively. The effect size showed that Perceived Susceptibility has no effect size ($f^2 < 0.0$). Meanwhile, Trust was found to have a medium effect ($f^2 > 0.15$) on HIS security policies compliance behaviour, while others had a small effect ($f^2 <= 0.2$).

The power analysis was also tested using the Daniel Soper power analysis calculator (http://www.danielsoper.com/statcalc3/calc.aspx?id=9). The power analysis result shows that P =1.0 (post hoc power analysis is acceptable if power value > 0.80). Thus, the path analysis is acceptable based on the power analysis value. The statistical results of PR, effect size and power analysis are shown in Table 4.11.

Table 4.11: Statistical results of predictive relevance, effect size and power analysis

Constructs	**Q²**	**q²**	**PR Impact**	***f*²**	**Effect size**	**Stats Power Analysis**
HIS security policies compliance behaviour	0.44				-	1.0
Perceived Benefit	0.09	0.05	Weak	0.08	Small	
Perceived Severity	0.13	0.00	No impact	0.01	Small	
Perceived Susceptibility	0.12	0.00	No impact	0.00	No effect	
Self-Efficacy	0.14	0.01	Weak	0.02	Small	
Management Support	-	0.01	Weak	0.02	Small	
Trust		0.13	Weak	0.24	Medium	
Perceived Barriers		0.02	Weak	0.01	Small	

4.5 Supplementary Study: Multi-Group Analysis

4.5.1 Measurement Model

The HIS usage experience group items loadings and cross loadings show that all the indicators in the high experience sample met the 0.7 standardised loading prescribed by Chin (1998) as shown in Table 4.12. Meanwhile, some of the indicators in the low experience sample scored factor loadings below 0.7. However, the factor loadings value scored higher on the intended constructs than any other constructs in both group models. This indicated that, individually, the measurement items were adequate in their validity.

Table 4.12: Multi-group items loading and cross loading

Items	High experience group								Low experience group							
	MS	PBAR	PBEN	PSEV	PSUS	TRUST	SE	UCB	MS	PBAR	PBEN	PSEV	PSUS	PTRUST	SE	UCB
MS01	**0.816**	-0.015	0.344	0.307	0.317	0.376	0.356	0.436	**0.721**	0.004	0.354	0.340	0.323	0.394	0.276	0.406
MS03	**0.764**	0.015	0.273	0.500	0.429	0.442	0.409	0.387	**0.662**	0.012	0.252	0.347	0.310	0.350	0.221	0.361
MS04	**0.787**	-0.100	0.359	0.415	0.413	0.492	0.370	0.440	**0.749**	-0.019	0.335	0.372	0.383	0.446	0.333	0.525
MS05	**0.772**	-0.006	0.194	0.264	0.258	0.341	0.331	0.364	**0.800**	0.100	0.236	0.292	0.331	0.441	0.344	0.435
MS06	**0.710**	-0.069	0.147	0.241	0.153	0.339	0.359	0.320	**0.762**	0.018	0.255	0.223	0.306	0.465	0.304	0.465
MS07	**0.673**	-0.052	0.153	0.254	0.065	0.380	0.202	0.236	**0.687**	0.011	0.198	0.212	0.237	0.467	0.280	0.375
MS08	**0.790**	-0.029	0.138	0.286	0.149	0.344	0.286	0.228	**0.760**	0.010	0.229	0.195	0.250	0.447	0.304	0.416
MS09	**0.746**	-0.135	0.212	0.238	0.182	0.452	0.323	0.363	**0.775**	0.078	0.332	0.291	0.358	0.539	0.381	0.456
MS10	**0.757**	0.001	0.249	0.361	0.266	0.387	0.391	0.380	**0.806**	0.075	0.303	0.368	0.350	0.367	0.331	0.426
MS11	**0.795**	-0.062	0.261	0.302	0.281	0.401	0.373	0.348	**0.801**	0.067	0.354	0.358	0.356	0.446	0.419	0.464
MS12	**0.787**	-0.084	0.226	0.410	0.309	0.355	0.322	0.316	**0.781**	0.124	0.349	0.452	0.394	0.398	0.400	0.434
MS13	**0.792**	-0.020	0.313	0.393	0.335	0.416	0.482	0.428	**0.716**	0.079	0.358	0.410	0.379	0.369	0.523	0.387
MS14	**0.855**	-0.143	0.371	0.424	0.351	0.489	0.430	0.453	**0.781**	-0.013	0.452	0.395	0.437	0.499	0.459	0.456
MS15	**0.746**	-0.162	0.183	0.241	0.159	0.416	0.405	0.370	**0.768**	0.116	0.169	0.232	0.220	0.362	0.314	0.431

Items	High experience group								Low experience group							
	MS	PBAR	PBEN	PSEV	PSUS	TRUST	SE	UCB	MS	PBAR	PBEN	PSEV	PSUS	PTRUST	SE	UCB
MS16	**0.783**	0.044	0.315	0.272	0.282	0.373	0.370	0.376	**0.770**	0.113	0.360	0.386	0.398	0.352	0.397	0.450
MS17	**0.797**	0.005	0.273	0.253	0.263	0.316	0.381	0.328	**0.803**	0.063	0.338	0.414	0.396	0.350	0.401	0.431
MS18	**0.826**	0.028	0.314	0.313	0.320	0.376	0.432	0.386	**0.777**	0.101	0.289	0.336	0.349	0.370	0.451	0.480
PBAR27	-0.151	**0.711**	0.008	-0.083	0.006	-0.101	0.092	-0.108	-0.029	**0.502**	-0.019	-0.028	-0.033	0.118	0.160	-0.022
PBAR32	0.048	**0.817**	-0.141	-0.050	0.026	-0.168	0.278	-0.109	0.134	**0.620**	-0.007	-0.014	-0.027	-0.002	0.230	-0.001
PBAR33	-0.041	**0.900**	-0.084	-0.163	-0.062	-0.213	0.155	-0.143	0.086	**0.983**	-0.080	-0.060	-0.123	-0.108	0.142	-0.107
PBEN35	0.316	-0.142	**0.769**	0.484	0.462	0.526	0.277	0.536	0.380	-0.152	**0.720**	0.512	0.538	0.511	0.242	0.566
PBEN36	0.353	-0.137	**0.848**	0.450	0.408	0.494	0.187	0.569	0.296	-0.133	**0.818**	0.527	0.497	0.467	0.253	0.534
PBEN37	0.229	-0.050	**0.821**	0.394	0.330	0.342	0.308	0.432	0.326	-0.021	**0.745**	0.443	0.515	0.436	0.338	0.378
PBEN38	0.265	-0.055	**0.846**	0.301	0.306	0.359	0.183	0.459	0.304	0.037	**0.837**	0.465	0.509	0.377	0.305	0.418
PBEN39	0.288	-0.030	**0.870**	0.288	0.306	0.380	0.158	0.486	0.297	-0.069	**0.847**	0.499	0.519	0.440	0.275	0.451
PBEN40	0.213	-0.004	**0.815**	0.328	0.283	0.401	0.247	0.460	0.318	0.021	**0.762**	0.404	0.379	0.439	0.355	0.379
PSEV25	0.492	-0.074	0.379	**0.819**	0.507	0.431	0.297	0.441	0.418	-0.037	0.568	**0.803**	0.660	0.419	0.256	0.456
PSEV28	0.333	-0.107	0.363	**0.875**	0.404	0.549	0.331	0.480	0.395	-0.039	0.476	**0.884**	0.468	0.403	0.372	0.475
PSEV29	0.210	-0.154	0.424	**0.833**	0.438	0.489	0.237	0.438	0.300	-0.084	0.492	**0.843**	0.513	0.324	0.304	0.401
PSUS19	0.283	0.034	0.328	0.437	**0.816**	0.337	0.239	0.281	0.426	-0.028	0.497	0.503	**0.872**	0.433	0.313	0.405

Items	High experience group								Low experience group							
	MS	PBAR	PBEN	PSEV	PSUS	TRUST	SE	UCB	MS	PBAR	PBEN	PSEV	PSUS	PTRUST	SE	UCB
PSUS20	0.346	0.073	0.259	0.403	**0.866**	0.361	0.190	0.348	0.406	-0.090	0.489	0.526	**0.878**	0.446	0.325	0.385
PSUS21	0.296	0.061	0.342	0.438	**0.828**	0.301	0.166	0.365	0.410	-0.092	0.613	0.678	**0.880**	0.488	0.323	0.473
PSUS24	0.261	-0.192	0.450	0.469	**0.754**	0.352	0.170	0.492	0.319	-0.212	0.567	0.522	**0.805**	0.447	0.274	0.416
TRUST41	0.502	-0.125	0.499	0.558	0.376	**0.882**	0.364	0.630	0.452	0.028	0.565	0.423	0.444	**0.798**	0.343	0.533
TRUST42	0.411	-0.164	0.398	0.527	0.333	**0.886**	0.254	0.618	0.473	-0.036	0.414	0.379	0.444	**0.880**	0.326	0.573
TRUST43	0.465	-0.198	0.521	0.565	0.444	**0.926**	0.305	0.727	0.462	-0.123	0.535	0.414	0.465	**0.913**	0.360	0.644
TRUST44	0.447	-0.234	0.403	0.416	0.322	**0.879**	0.295	0.634	0.515	-0.115	0.485	0.385	0.489	**0.894**	0.386	0.636
SE22	0.365	0.196	0.266	0.184	0.212	0.205	**0.821**	0.262	0.374	0.022	0.367	0.359	0.398	0.272	**0.802**	0.363
SE23	0.488	0.184	0.207	0.232	0.191	0.248	**0.811**	0.309	0.464	0.167	0.315	0.300	0.330	0.352	**0.816**	0.379
SE30	0.304	0.173	0.229	0.415	0.205	0.350	**0.822**	0.393	0.226	0.194	0.216	0.266	0.129	0.281	**0.704**	0.313
SE31	0.406	0.148	0.199	0.313	0.158	0.318	**0.844**	0.322	0.403	0.138	0.240	0.231	0.230	0.352	**0.791**	0.392
UCB45	0.410	-0.194	0.545	0.468	0.375	0.684	0.298	**0.873**	0.471	-0.117	0.568	0.460	0.449	0.643	0.390	**0.808**
UCB46	0.401	-0.130	0.595	0.511	0.433	0.691	0.303	**0.889**	0.447	-0.117	0.534	0.566	0.492	0.580	0.390	**0.851**
UCB47	0.427	-0.097	0.482	0.506	0.458	0.600	0.376	**0.873**	0.506	-0.014	0.396	0.368	0.330	0.493	0.364	**0.820**
UCB48	0.451	-0.102	0.485	0.415	0.384	0.608	0.412	**0.902**	0.473	-0.074	0.413	0.328	0.319	0.524	0.390	**0.812**

Legends:MS – Management Support; PBAR – Perceived Barrier; PBEN – Perceived Benefit; PSEV – Perceived Severity; PSUS – Perceived Susceptibility; TRUST – Trust; SE – Self-Efficacy; UCB– HIS security policies compliance behaviour.

All the constructs in HIS experience groups model satisfy the requirements for convergence validity (CR greater than 0.7) and AVE greater than 0.5. In the high experience sample (Table 4.13a), the CR values ranged from 0.853 to 0.963 and the values of AVE ranged from 0.604 to 0.782. Meanwhile, the values of CR (0.760 to 0.959) and AVE (0.534 to 0.761) in the low experience sample (Table 4.13b) were slightly lower than in the high experience sample. However, the results for both of the measurement models for each group showed that all seven constructs are valid measures based on their parameter estimates and statistical significance (Hair et al., 2010, 2013).

Meanwhile, the CA values in high experience sample (Table 4.13a) ranged from 0.739 to 0.959 while in the low experience sample (Table 4.13b); the CA values ranged from 0.674 to 0.954. The CA results were acceptable because they all exceeded 0.7 except for the Perceived Barrier construct in the low experience sample, as shown in Table 4.13 (a-b).

Table 4.13: Convergent and reliability validity for multi-group model

(a) High Experience Model

				Correlation of constructs							
	Cronbach's	**Composite**									
Models/Constructs	**Alpha (α)**	**Reliability**	**AVE**	**MS**	**PBAR**	**PBEN**	**PSEV**	**PSUS**	**TRUST**	**SE**	**UCB**
High Experience											
MS	0.959	0.963	0.604	**0.777**							
PBAR	0.739	0.853	0.661	-0.057	**0.813**						
PBEN	0.909	0.929	0.687	0.341	-0.090	**0.829**					
PSEV	0.798	0.880	0.710	0.427	-0.128	0.458	**0.842**				
PSUS	0.834	0.889	0.668	0.363	-0.018	0.429	0.538	**0.817**			
TRUST	0.916	0.940	0.798	0.511	-0.203	0.512	0.579	0.416	**0.893**		
SE	0.844	0.895	0.680	0.481	0.212	0.271	0.347	0.232	0.341	**0.825**	
UCB	0.907	0.935	0.782	0.477	-0.149	0.599	0.538	0.467	0.733	0.390	**0.884**

(b) Low Experience Model

							Correlation of constructs				
	Cronbach's	**Composite**									
Models/Constructs	**Alpha (α)**	**Reliability**	**AVE**	**MS**	**PBAR**	**PBEN**	**PSEV**	**PSUS**	**TRUST**	**SE**	**UCB**
Low Experience											
MS	0.954	0.959	0.579	**0.761**							
PBAR	*0.674*	0.760	0.534	0.074	**0.731**						
PBEN	0.879	0.908	0.624	0.410	-0.077	**0.790**					
PSEV	0.798	0.881	0.712	0.446	-0.061	0.609	**0.844**				
PSUS	0.882	0.919	0.738	0.456	-0.119	0.631	0.651	**0.859**			
TRUST	0.895	0.927	0.761	0.545	-0.076	0.571	0.457	0.528	**0.872**		
SE	0.786	0.861	0.608	0.485	0.163	0.369	0.369	0.360	0.406	**0.779**	
UCB	0.842	0.894	0.677	0.574	-0.102	0.588	0.530	0.490	0.686	0.467	**0.823**

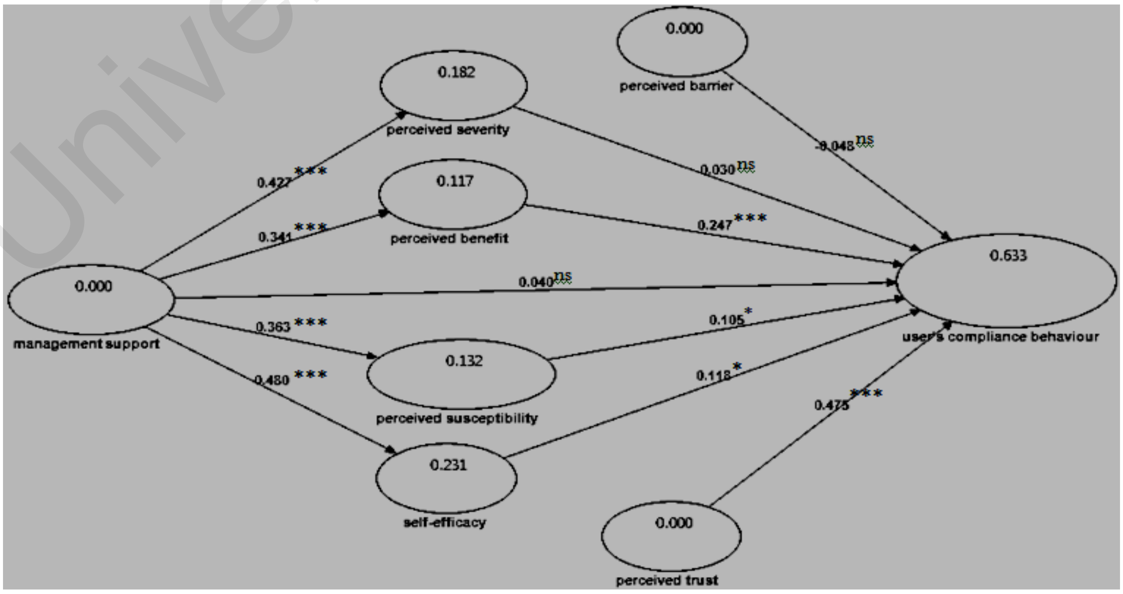
Note: Diagonal elements in the 'correlation of constructs' matrix are the square root of average variance extracted (AVE). For adequate discriminant validity, diagonal should be greater than corresponding off-diagonal elements.
Legends: MS – Management Support; PBAR – Perceived Barrier; PBEN – Perceived Benefit; PSEV – Perceived Severity; PSUS – Perceived Susceptibility; TRUST – Trust; SE – Self-Efficacy; UCB – HIS security policies compliance behaviour.

4.5.2 Structural Model for Multi-Group

a) Moderating Effect of Health Information System (HIS) Experience

To test the moderating effect of HIS experience among health professionals, this study estimated two separate models in PLS: the high experience group and the low experience group. The differences across the two models were tested using the test for difference suggested by Chin and Dibbern (2010). To evaluate the predictive power of the structural models, the R^2 was calculated for users' compliance behaviour with ISPs of HIS. The results suggested that distinct of some antecedents influence users' compliance behaviour with HIS security policies within each HIS experience group.

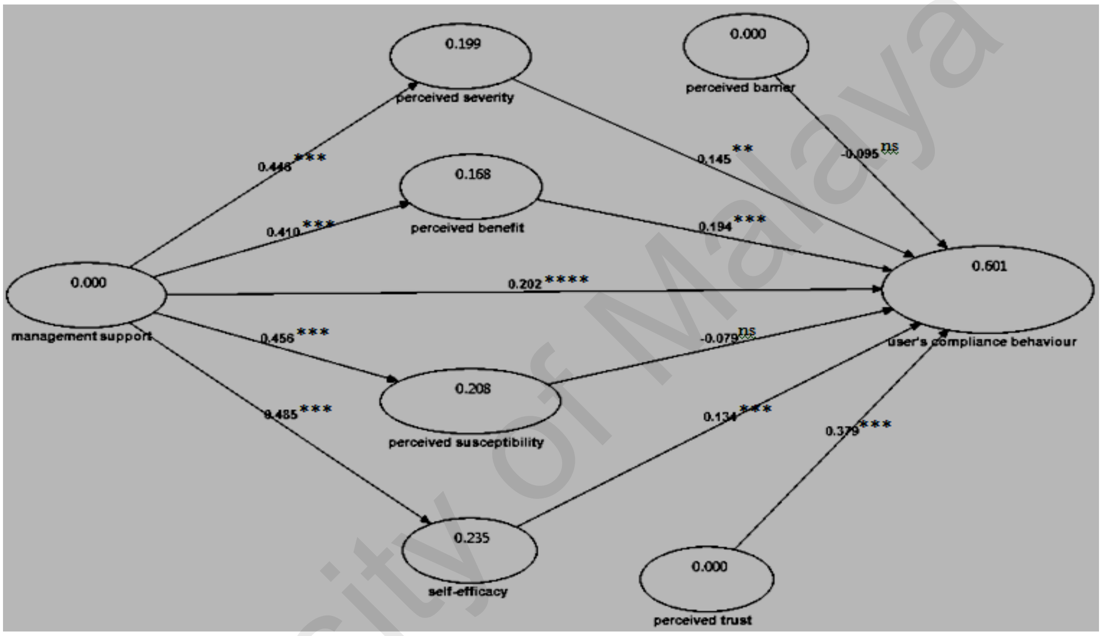
Higher explanatory power has favoured users with higher HIS experience by contributing 63 percent of variations in compliance behaviour towards HIS security policies as shown in Figure 4.3. It was mainly influenced By Perceived Benefits (β = 0.247***), Trust (β = 0.475***), Self-Efficacy (β = 0.118*), and Perceived Susceptibility (β = 0.105*).



Note: *p < 0.1, **p < 0.05, ***p < 0.01, ns – not significant

Figure 4.3: High Experience Model

Meanwhile, users with lower HIS experience by contributing 60 percent of variations in compliance behaviour towards HIS security policies as shown in Figure 4.4. In contrast, the users with lower experience was mainly influenced By Perceived Benefits (β = 0.194***), Trust (β = 0.379***), Self-Efficacy (β = 0.134**), Management Support (β = 0.202***) and Perceived Severity (β = 0.145**).



Note: *p < 0.1, **p < 0.05, ***p < 0.01, ns – not significant

Figure 4.4: Low Experience Model

Even though, the HIS experience significantly moderates the positive associations between Perceived Benefits, Trust, Self Efficacy and user's compliance behaviour towards HIS security policies on both models, there were no significant differences between stated variables and HIS experience through a comparison test by Chin and Dibbern (2010).

The findings showed that Perceived Susceptibility and Management Support have favoured compliance behaviour towards HIS security policies among health professional with higher HIS experience through a test of differences by Chin and Dibbern (2010). It has supported the formulated hypothesis due to the fact that lower experienced health professionals are dealing with system catch up where as those with higher experiences of HIS usage favour innovation catch up (Table 4.14). Thus, *H9, H10 and H11* were rejected while *H12* was accepted. Moreover, *H8* was only supported for perceived susceptibility (*H8c*) as shown in Table 4.14.

Table 4.14: Statistical comparisons of standard path coefficient

Hypotheses	Path	High experience group (n = 226)		Low experience group (n = 228)		Statistical Comparisons of Path
		Standard Path Coefficient	**Standard Error**	**Standard Path Coefficient**	**Standard Error**	
H8(a)	PBEN --> UCB	*0.247*	0.056	*0.195*	0.070	0.581 (Rejected)
H8(b)	PSEV --> UCB	0.024	0.068	*0.143*	0.068	1.240 (Rejected)
H8(c)	PSUS --> UCB	*0.105*	0.067	-0.075	0.080	*1.823* (Accepted)*
H9	PBAR --> UCB	-0.060	0.044	-0.085	0.070	0.302 (Rejected)
H10	TRUST --> UCB	*0.468*	0.053	*0.378*	0.059	1.137 (Rejected)
H11	SE --> UCB	*0.126*	0.072	*0.131*	0.050	0.057 (Rejected)
H12	MS --> UCB	0.035	0.055	*0.195*	0.058	*2.001** (Accepted)*

Note: Italic values represent the standard path coefficient is significant for each model of the groups. Significance value of two tailed (Hair, et al., 2011): *p < 0.1, t >= 1.65; **p < 0.05, t >= 1.96; ***p < 0.01, t => 2.58
Legends: MS – Management Support; PBAR – Perceived Barrier; PBEN – Perceived Benefit; PSEV – Perceived Severity; PSUS – Perceived Susceptibility; TRUST –Trust; SE – Self-Efficacy; UCB – HIS security policies compliance behaviour

4.5.3 Predictive Relevance (PR), effect Size and Power Analysis of Multi-Group Model

The predictive relevance of the multi-group model was also tested using the blindfolding technique. Same blindfolding procedure has been used for both of multi-group model (High Experience Model and Low Experience Model). The predictive relevan result for both groups has shown not much difference.

According to the results for the high experience model, as shown in Table 4.15, using an omission distance (D) of 7, this study obtains a Q^2 of 0.78, which is more than the cut-off value 0.0 (Hair et al., 2011, 2013), thereby indicating that the high experience model in this study has predictive relevance. The relative impact of the research model calculated by obtaining q^2 showed that all constructs have no relative impact except Perceived Trust ($q^2 = 0.16$) and Perceived Barrier ($q^2 = 0.76$), which indicated a medium and large impact. The effect size of f^2 showed that Perceived Susceptibility, Perceived Severity, Perceived Barrier and Management Support have no effect size ($f^2 < 0.00$). Meanwhile, Trust was found to have a medium effect ($f^2 > 0.30$) on HIS security policies compliance behaviour while Self-Efficacy had a small effect ($f^2 = 0.03$).

For the low experience model, as shown in Table 4.16, using an omission distance (D) of 7, this study obtains a Q^2 of 0.69, thereby indicating that the low experience model in this study has predictive relevance. The relative impact of the research model calculated by obtaining q^2 showed that all constructs have no relative impact except Trust ($q^2 = 0.16$) and Perceived Barrier ($q^2 = 0.74$), which indicated a medium and large impact. The effect size of f^2 showed that all the constructs were founds to have a small effect on HIS security policies compliance behaviour except Trust, which has medium effect ($f^2 = 0.20$).

The power analysis was also tested using the Daniel Soper power analysis calculator (http://www.danielsoper.com/statcalc3/calc.aspx?id=9). The power analysis result shows that P =1.0 (post hoc power analysis is acceptable if power value > 0.80). Thus, the path analysis for both multi-group models is acceptable based on the power analysis value.

Table 4.15: Statistical results of predictive relevance, effect size and power analysis for high experience model

Constructs	**Q^2**	**q^2**	**PR Impact**	**f^2**	**Effect size**	**Stats Power Analysis**
HIS security policies compliance behaviour	0.78				-	1.0
Perceived Benefit	0.67	0.00	No impact	0.11	Small	
Perceived Severity	0.71	0.00	No impact	0.00	No effect	
Perceived Susceptibility	0.68	0.00	No impact	0.00	No effect	
Self-Efficacy	0.68	0.00	No impact	0.03	Small	
Management Support		0.00	No impact	0.00	No effect	
Trust		0.16	Medium	0.30	Medium	
Perceived Barriers		0.76	Large	0.00	No effect	

Table 4.16: Statistical results of predictive relevance, effect size and power analysis for low experience model

Constructs	Q²	q²	PR Impact	*f*²	Effect size	Stats Power Analysis
HIS security policies compliance behaviour	0.69				-	1.0
Perceived Benefit	0.61	0.00	No impact	0.05	Small	
Perceived Severity	0.70	0.00	No impact	0.03	Small	
Perceived Susceptibility	0.74	0.00	No impact	0.01	No effect	
Self-Efficacy	0.60	0.00	No impact	0.03	Small	
Management Support		0.00	No impact	0.05	Small	
Trust		0.16	Medium	0.20	Medium	
Perceived Barriers	0.74	Large	0.02	Small		

4.6 Discussion on PLS-SEM Findings

This study has added up some values to Ng et al. (2009) through the multidimensional extension of constructs using multidisciplinary theories (TPB, HBM and Trust) to explain the complexity of human values in maintaining the security effectiveness in the Malaysian context. Moreover, this study may be the first to conduct the mediation effect of health professionals' information security awareness based on the constructs adapted from HBM (Perceived Severity, Percieved Susceptibility and Perceived Benefit) and Self-Efficacy (PCB) in the relationship between management support and HIS security policies compliance behaviour in the public health institution in Malaysia. Health professionals who are also HIS users might have a different perspective concerning information security, but practicing information security behaviour is the responsibility of the employees.

In addition, this study also found that Trust and security barriers have received scant attention in information security behaviour studies, especially in the healthcare sector. Trust in an organization's ISPs can improve compliance behaviour while barriers towards complying with ISPs cause non-compliance behaviour among employees (Brady, 2011). Without proper knowledge of information security, lack of confidence and the necessary skills to practice information security mechanisms, employees will not be able to utilize ISPs appropriately.

The quantitative research findings were discussed further as following:

4.6.1 Development of HISSPC Model

Research objective (RO1) leads to the development of the Health Information System Security Policies Compliance (HISSPC) Model (RO2). RO1 was achieved through an extensive review of previous literature. The current study found that previous empirical studies employed several behaviour models adapted from, among others, the Protection Motivation Theory (PMT) (Ifinedo, 2012; Herath & Rao, 2009b), Theory of Planned Behaviour (TPB) (Warkentin et al., 2011; Bulgurcu et al., 2010a; Siponen et al., 2010), Rational Choice Theory (RCT) (Bulgurcu et al., 2010a; Li et al., 2010), Health Belief Model (HBM) (Ng et al., 2009) and Deterrence Theory (Herath & Rao, 2009b; Straub, 1990), among others. These behavioural models were significant and valid based on previous analysis, and many highlighted human factor issues, such as threat appraisal, technology barrier and self-efficacy.

However, there has been a lack of studies in the healthcare sector exploring the importance of management support, especially leadership behaviour, security barrier and trust factor, in investigating health professionals' compliance behaviour towards HIS security policies. Hence, the current study reviewed several constructs that are related to the management support dimension and how this dimension can affect users' information security awareness and compliance behaviour towards HIS security policies. In doing this, the TPB, HBM and Trust factor were integrated to develop the HISSPC Model.

4.6.2 The Significant Factors of HISSPC Model

In answering RQ2, several sub-questions were developed. This study also addressed twelve (12) research hypotheses to answer all the sub-questions under RQ2. The convergence and discrimant validity test has been conducted for all models in this study and the results were acceptable for testing the structural model. The summary of an assessment of reflective measurement model is shown in Table 4.17 and research hypotheses testing results are shown in Table 4.18. Meanwhile, the summary of statistical path results of HISSPC model is shown in Figure 4.5, whereby the solid arrow shows the significant effect between the indicated factors and dependent variable while the dash arrow shows no effect.

Table 4.17: Assessment of reflective measument model

Validity Type	Criterion	Results
Unidimensionality	EFA	An item loading is usually considered high if the loading coefficient is above .60 and considered low if the coeeficient is below .040 (Gefen and Straub, 2005). Using PCA with varimax rotation, the seven constructs (Management Support, Perceived Severity, Perceived Benefit, Perceived Susceptibility, Self-Efficacy, Perceived Barrier and Trust) were retained in this study, which explained approximately 68% of the total variance (eigenvalues greater than 1).
Internal consistency reliability	Croanbach's alpha (CA)	The CA value is acceptable if greater than 0.7 (Hair et al., 2010). In this study, the CA values ranged from 0.713 to 0.957 (Full Model), 0.798 to 0.959 (High Experience Model) and 0.674 to 0.954 (Low Experience Model, which is acceptable based on Hair et al. (2010).
	Composite reliability (CR)	The CR value for each constructs ranged from 0.837 to 0.964 (Full Model), 0.853 to 0.963 (High Experience Model) and 0.760 to 0.959 (Low Experience Model), which exceeded the recommended value of 0.7 (Hair et al., 2010).
Indicator reliability	Indicator loadings	This study used a cut-off value of 0.7 or higher loadings to be considered significant (Hair et al., 2010). The results shown that most of the indicators measuring a particular construct had loading values more than 0.7 on their respective constructs for all models.
Convergent validity	Average variance extracted (AVE)	The AVE value for each construct ranged between 0.590 and 0.727 (Full Model), 0.604 and 0.798 (High Experience Model), while for Low Experience Model, the value ranged between 0.534 and 0.761, which is greater than 0.5; thus, the cut-off values ensure that at least 50% of the variances in the construct were explained by the set of indicators.
Discriminant validity	Cross-loadings	All the loading of each indicator is higher for its designated construct than for any of the other constructs, and each of the constructs loads highest with its own items, it can be inferred that the models' constructs differ sufficiently from one another (Chin, 1998).
	Fornell-Larcker criterion	Fornell and Larcker (1981) suggest that discriminant validity is established if a latent variable accounts for more variance in its associated indicator variables than it shares with other constructs in the same model. To satisfy this requirement, each construct's AVE must be compared with its squared correlations with other constructs in the model. The research findings show that the squared correlation values were higher than the values in the row and column (Table 4.8, Table 4.13a and Table 4.13b), indicating adequate dscriminant validity.
Predictive Relevance	Blinfolding procedure	The blindfolding technique omits data for a given block of indicators and then predicts the omitted part based on the calculated parameters. Using an omission distance (D) of 7, this study obtain stone-geisser (Q2) value of 0.44 (Full Model), 0.78 (High Experience Model) and 0.69 (Low Experiene Model), which is than the cut-off value 0.0 (Hair et al., 2013), thus indicating all models in this study have predictive relevance.
Effect Size (f^2) and Power Analysis	Stone-Geisser	Chin (1998, p. 317) stated that the higher the f^2, the greater the influence of the exogenous construct whereby values of 0.02, 0.15 and 0.35 can be respectively regarded as small, medium or large effect respectively.

Validity Type	Criterion	Results
		Full Model: The effect size showed that Perceived Susceptibility has no effect size ($f2 < 0.0$). Meanwhile, Trust was found to have a medium effect ($f2 > 0.15$) on HIS security policies compliance behaviour, while others had a small effect ($f2 <= 0.2$). **High Experience Model:** The effect size of f^2 showed that Perceived Susceptibility, Perceived Severity, Perceived Barrier and Management Support have no effect size ($f^2 < 0.00$). Meanwhile, Trust was found to have a medium effect ($f^2 > 0.30$) on HIS security policies compliance behaviour while Self-Efficacy had a small effect ($f^2 = 0.03$). **Low Experience Model:** The effect size of f^2 showed that all the constructs were founds to have a small effect on HIS security policies compliance behaviour except Trust, which has medium effect ($f^2 = 0.20$).

Table 4.18: Summary of hypotheses testing results

Research Hypotheses	Results
RQ2.1: To what extend does the indicated factor in the HISSPC Model influences users' compliance behaviour towards HIS security policies?	
H1(a): Perceived benefit will have a positive effect on HIS security policies compliance behaviour.	Accepted
H1(b): Perceived severity will have a positive effect on HIS security policies compliance behaviour.	Accepted
H1(c): Perceived susceptibility will have a positive effect on HIS security policies compliance behaviour.	Rejected
H2: Perceived barrier will have a positive effect on HIS security policies compliance behaviour.	Accepted
H3: Perceived trust will have a positive effect on HIS security policies compliance behaviour.	Accepted
H4: Self-efficacy will have a positive effect on HIS security policies compliance behaviour.	Accepted
H5: Management support will have a positive effect on HIS security policies compliance behaviour.	Accepted
H6(a): Management support will have a positive effect on perceived benefit.	Accepted
H6(b): Management support will have a positive effect on perceived severity.	Accepted
H6(c): Management support will have a positive effect on perceived susceptibility.	Accepted

Research Hypotheses	Results
RQ2.2: To what extent does the intervening factor in the HISSPC Model influence users' compliance behaviour towards HIS security policies?	
H6(d): Management support will have a positive indirect effect on HIS security policies compliance behaviour through perceived benefit.	Accepted
H6(e): Management support will have a positive indirect effect on HIS security policies compliance behaviour through perceived severity.	Accepted
H6(f): Management support will have a positive indirect effect on HIS security policies compliance behaviour through perceived susceptibility.	Rejected
H7(a): Management support will have a positive effect on self-efficacy.	Accepted
H7(b): Management support will have a positive indirect effect on HIS security policies compliance behaviour through self-efficacy.	Accepted
RQ2.3: To what extent does the HIS experience level of user moderate the influence of the factors in the HISSPC Model on users' compliance behaviour towards HIS security policies?	
H8(a): High experience users significantly moderate the positive relationship between perceived benefit and compliance behaviour towards HIS security policies.	Rejected
H8(b): High experience users significantly moderate the positive relationship between perceived severity and compliance behaviour towards HIS security policies.	Rejected
H8(c): High experience users significantly moderate the positive relationship between perceived susceptibility and compliance behaviour towards HIS security policies.	Accepted
H9: High experience users significantly moderate the positive relationship between perceived barriers and compliance behaviour towards HIS security policies.	Rejected
H10: High experience users significantly moderate the positive relationship between perceived trust and compliance behaviour towards HIS security policies.	Rejected
H11: High experience users significantly moderate the positive relationship between self-efficacy and compliance behaviour towards HIS security policies.	Rejected
H12: Low experience users significantly moderate the positive relationship between management support and compliance behaviour towards HIS security policies.	Accepted
Research Hypotheses for Moderation-Mediation effect for Multi-group Analysis	
Low experience users significantly moderate the positive relationship between management support and compliance behaviour towards HIS	Rejected

Research Hypotheses	Results
security policies through perceived benefit.	
Low experience users significantly moderate the positive relationship between management support and compliance behaviour towards HIS security policies through perceived severity.	Rejected
Low experience users significantly moderate the positive relationship between management support and compliance behaviour towards HIS security policies through perceived susceptibility.	Rejected
Low experience users significantly moderate the positive relationship between management support and compliance behaviour towards HIS security policies through self-efficacy.	Rejected

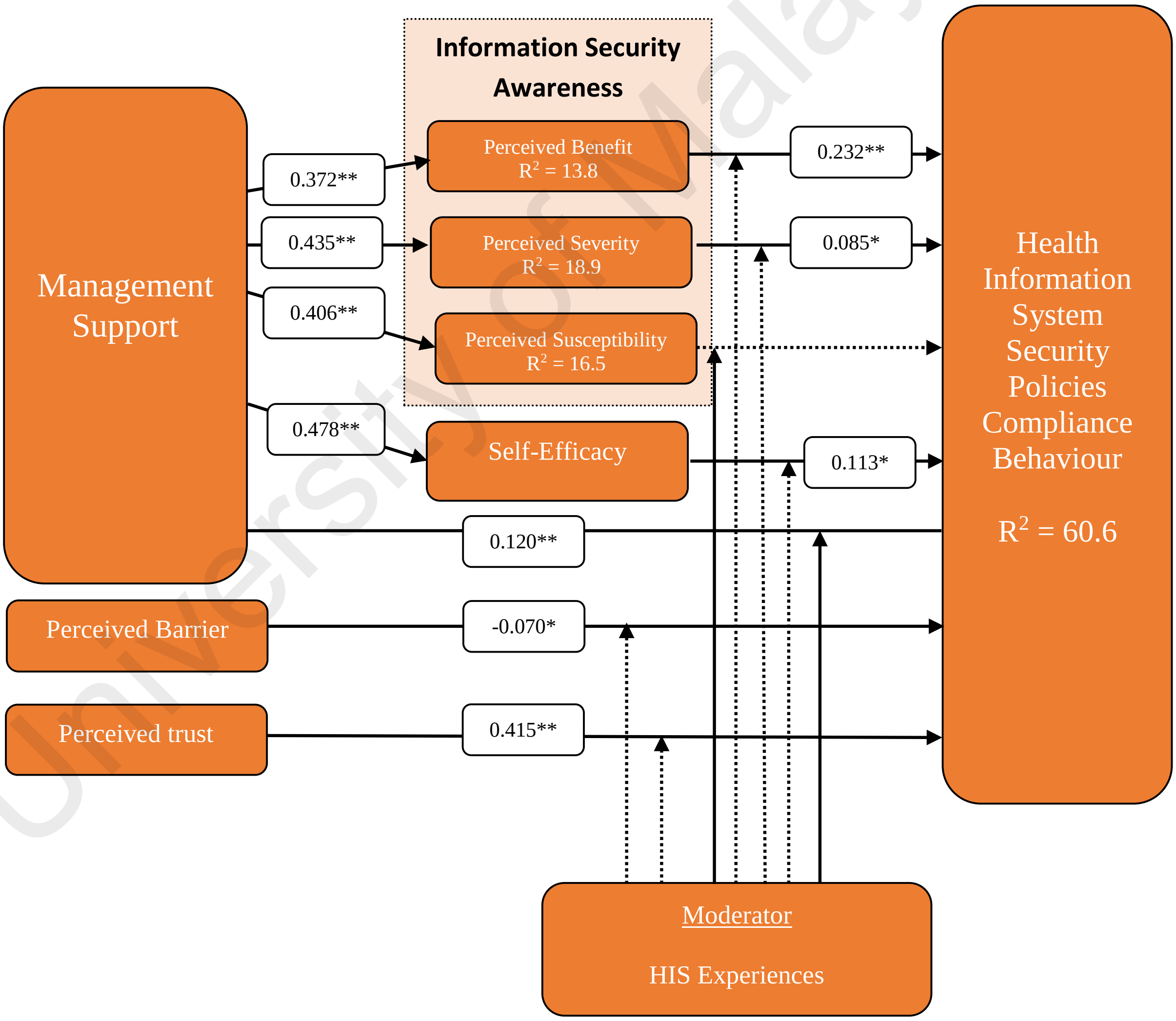


Figure 4.5: The statistical path results of HISSPC Model

4.6.2.1 Outcomes of Health Professional’s Information Security Awareness

The PLS-SEM path analysis revealed that most of the information security awareness constructs in the HISSPC Model affected health professionals’ compliance behaviour towards HIS security policies except for Perceived Susceptibility. Perceived Severity and Perceived Benefit are consistent with the nature of security, as the motivation for security is to mitigate risks and reduce the likelihood of threats (Ng et al., 2009). Perceived Severity in the current study was used to measure health professionals’ awareness towards the severity of information security threats. The current finding is consistent with the findings in previous studies, perceived that the severity affects users’ intention to comply with ISPs (Vance et al., 2012; Son, 2011).

Herath and Rao (2009a) suggested that if employees perceive higher levels of penalties for non-compliance with ISPs, such as loss of job or heavy fines, their non-compliance behaviour is likely to decrease. It is believed that if the end-users of HIS are aware of the severity of information security threats, then they can prevent such a threat from happening. Moreover, management should enforce the consequences of not complying with the rules and regulations related to information system use, such as severe penalties. Employees will adhere if they need to avoid any embarrassment of wrongdoing and if they fear the penalties (Siponen et al., 2014; Warkentin et al., 2011).

Meanwhile, Perceived Benefit was used to measure users’ awareness towards the benefits of using security-countermeasure in their daily tasks; this is somewhat different from the measurement items used in previous studies (Siponen et al., 2010; Ng et al., 2009). Nevertheless, in line with many previous studies, it was found that Perceived Benefit influences compliance behaviour towards ISPs (Hovav & D’Arcy, 2012;

Bulgurcu et al., 2009; Hagen et al., 2008). Awareness of security-countermeasures play an important role in increasing users' compliance behaviour towards ISPs in health institutions since health professionals will be less likely engage in insecure behaviour if they are aware of the benefit of using the security tools that are provided in the institutions. This is supported by D'Arcy et al. (2009), who indicated that if users perceive the benefit of security-countermeasure it can prevent security threats if users know how to use it properly. Information security training is one of the methods to increase employee's information security awareness towards the benefit of applying security-countermeasures in preventing information security threats (Renaud, 2012). Therefore, we suggest that management should implement effective information security training programmes for all employees in the organization and that attendance should be made compulsory.

On the other hand, Perceived Susceptibility does not seem to affect health professionals' behaviour towards complying with ISPs of HIS. This is consistent with the research findings of Vance et al. (2012), who reported that most of their respondents did not believe that they would be subjected to information security threats if they did not comply with their organisation's ISPs. This may be because employees do not experience security threats or are less likely to experience them (Johnston & Warkentin, 2010). Health professionals had similar perceptions whereby they did not find health data to be susceptible to security risks. However, Ng et al. (2009) found that Perceived Susceptibility was a determinant of computer security behaviour. Their study showed that most of the respondents agreed that files, or any documents attached to an email were vulnerable with security threats, such as viruses. Thus, the current study suggested that this issue needs to be investigated further as the scope of this study is limited to health professionals working at three government hospitals.

4.6.2.2 Outcomes of Trust

The effect of Trust on health professional's behaviours towards HIS security policies was the most significant predictor among the constructs, which is in line with Williams (2008). Thus, the hospital management must ensure that HIS security policies are effectively documented and distributed to all employees in the hospitals. The ISP documents must be easy to understand and presented in simple language in order for employees to feel confident with the security guidelines, so that they are able to practice them as recommended by the Malaysian Ministry of Health (MOH). A previous study suggested that communication about information security between the management and employees must be effective to influence employees trust (Koskosas et al., 2011). If trust is not established among the health professionals, the health care sector might face greater risks of security incidents. Therefore, the culture to inculcate trust in the organization must be embedded before implementing the ISPs.

4.6.2.3 Outcomes of Self-Efficacy

The current study also revealed that most of health professionals do not have confidence in their information security skills. Nevertheless, in line with previous studies, it is indicated that Self-Efficacy has a positive influence on employee's compliance behaviour towards ISPs (Brady, 2011; Herath & Rao, 2009b). Similarly, Self-Efficacy has also been found to significantly influence computer security behaviour, such as scanning files before downloading from an email or website (Ng et al., 2009; Rhee et al., 2009). Thus, hospital management must seriously consider this issue because the users of the information system (IS) must have the necessary skills to adopt information security tools as this can lead to the adequate practice of information security behaviour. Furthermore, it is essential that IS users are confident and able to perform the necessary mitigation process because it can reduce security incidents (Warkentin et al., 2011; Ng et al., 2009; Beas & Salanova, 2006).

4.6.2.4 Outcomes of Perceived Barrier

Perceived Barrier in the current study was used to measure health professionals' perception towards the difficulty of adopting HIS security policies. Although Ng et al. (2009) found that Perceived Barrier was not a determinant of human security behaviour, the current study found that Perceived Barrier constitute a negatively significant predictor when applied to HIS security policies compliance behaviour, and the majority of the respondents did not find many barriers or inconvenience in complying with the HIS security policies. It can be concluded that most of the HIS users are aware of their responsibility to protect the health data. They just need to be taught to practice information security behavior adequately. This can be done through effective education and learning.

4.6.2.5 Outcomes of Management Support

The structural analysis revealed that Management Support has a strong significant impact on health professionals' information security awareness in terms of the risk of information security threat (Perceived Susceptibility), the seriousness of the consequences of not complying with HIS security policies (Perceived Severity), the benefits of security-countermeasures in preventing information security threats (Perceived Benefit) and Self-Efficacy towards using security technology. Health professionals or HIS users in the current study believed that Management Support is important in preventing information security threats through leadership behaviour, and the implementation of information security training and awareness programmes in the health institutions.

The research findings of Cheng et al. (2013) indicated that when employees are aware of the severity and susceptibility of security threats, they can make a conscious decision to perform secure behaviour. They also argued that the relationship between management and employees is important to prevent information security threats from spreading in the organization. Further, according to Koskosas et al. (2011), employees must be proactive concerning information security. If the whole organization practices the recommended information security behaviour, the level of user awareness can be increased. It is also believed the information security behaviour might have an effect on the success or failure of the information security process in the organization, especially in the medical domain. Thus, the hospital management needs to control and monitor their employees' behaviour concerning information security because health information is sensitive and requires high confidentiality (Lechler et al., 2011).

Most of the respondents believed that good training and an effective security awareness programme could improve their compliance behaviour towards information security policies, as well as enhance their skill in using information security tools. Similarly, previous literature also showed that information security training and awareness programmes could increases users' self-efficacy (Huang et al., 2011), and significantly affect users' intention to comply with ISPs (Al-Omari et al., 2012a; Bulgurcu et al., 2010a).

Moreover, it is vital for organizations to conduct ongoing security training to ensure employees are always aware of the importance of information security (Hagen et al., 2008). Appropriate security training for employees is important because it can create and maintain a high level of information security awareness (Ifinedo, 2012; Bulgurcu et al., 2009; Puhakainen, 2006). A recent study also suggested that security awareness training is effective in decreasing violations towards an organization's ISPs (Barlow et al., 2013). Therefore, effective security training should be able to deliver messages about information security risks to all employees and teach them how to utilize security practices properly and the management of health institutions, such as hospital directors and hospital IT managers, must play a role in sorting out the problemsofhuman errors before developing security policies for the information system.

4.6.2.6 Outcomes of Mediation Effects (Information Security Awareness and Self-Efficacy)

To the best of our knowledge, neither the mediation effect of HBM constructs (Perceived Severity, Perceived Benefit and Perceived Susceptibility) have been covered in previous studies related to compliance behaviour towards HIS security policies, nor Self-Efficacy in the relationship between Management Support and HIS security policies compliance. The findings of the current study showed that all the intervening variables (Perceived Severity, Perceived Benefit and Self-Efficacy) mediated the effect in the relationship between the Management Support and users' compliance behaviour towards HIS security policies, while Perceived Susceptibility was shown to be insignificant.

In line with previous studies, management support in this study was found to be important in promoting information security awareness and enhancing the self-efficacy of information security among IS users (Al-Omari et al., 2012a; Warkentin et al., 2011; Brady, 2010). Therefore, we suggested that hospital management must possess definite knowledge concerning the importance of information security to create an organizational environment that is conducive to achieve security goals. Additionally, hospital management must always communicate with their employees and clearly state the hospitals' goals and career-promotion criteria, so that the employees will understand and appreciate the opportunities given to them.

According to previous studies, it is very difficult to monitor users' behaviour towards practicing information security appropriately (Box & Pottas, 2013; Debi, 2008). For example, in respect of the ISPs, it has already been stated that users need to change their password regularly and scan all devices before attaching it to the computer (Parsons et al., 2014). In most cases, users tend to ignore this, especially when they are busy and need to finish their work immediately. Sometime users do not feel that this action is necessary or that it violates the policy. This is happening because users do not have sufficient knowledge about information security threats (Parsons et al., 2014; Al-

Omari et al., 2012a). Thus, hospital management need to enforce this policy, as well as constantly remind their employees about the importance of practicing information security behaviour. Having good security technology is still not enough if a good security culture is not embedded in every department of the hospital.

Moreover, there are types of user who are not familiar with the information security tools. These people very much depend on the information technology staff. Empirically, the findings of this study suggests that a positive evaluation of information security training conducted by the health institutions might increase users' self-efficacy, and therefore, leads to improved users' compliance behaviour towards HIS security policies.

4.6.2.7 Outcomes of Moderator Effects (HIS Experience)

This study has also conducted the moderating analysis as a supplementary study. In doing so, the research models were tested separately to investigate the moderating effect of HIS experience among different groups of health professionals (high experience users and low experience users) in selected hospital to explain the impact of Management Support, Information Security Awareness constructs, Perceived Barriers, Trust and Self-Efficacy on health professionals' compliance behaviour towards HIS security policies.

The PLS-SEM analysis for full model group shows that Management Support influences all constructs in Information Security Awareness dimension, Self-Efficacy and user's compliance behaviour towards ISPs. The respondents believed that information security training and awareness programme are important. They also believed that good training and effective security awareness programme can improve their behaviour toward information security, as well as enhance their skills in using information security tools. Thus, Malaysian public hospital management personnel such as hospital directors and hospital information technology (IT) managers play an important role in sorting out problems of human errors before developing any policies related with information security. Moreover, organizations should invest and spend more in information security training and education to maintain information security awareness in hospitals.

Moreover, Perceived Susceptibility does not seem to affect user's behaviour towards complying with ISPs, while other HISSPC constructs (Perceived Severity, Perceived Benefit of security-countermeasure, Self-Efficacy, Management Support, Perceived Barrier and Trust) were significant. The majority of the respondents did not find health data to be susceptible to security risks, probably because they lack experience and were not familiar with security threats. They may also think that current security technology is able to protect health data. Therefore, it is very important to educate users about risks of information security threats. Users should be aware of the probability of information security threats that may exist in the organization (Perceived Susceptibility), and the consequences of information security threats to the employees and organization (Perceived Severity) if the threat exists (Mejias, 2012). In addition, users also must be able to identify information security threats (Thomson & von Solms, 2006), so that they would be able to adjust their action. However, this action is based on their decision, and employees make decisions based on their understanding of the subject (Kruger & Kearney, 2006). Previous studies have argued that if employees are not aware of their security actions, it may result in many security incidents (Cheng et al., 2013). Therefore, the management plays an important role in injecting the right knowledge about information security to all employees by conducting information security training and education, and implementing security awareness programmes or campaigns effectively.

Furthermore, Perceived Barrier was found to be insignificant in both groups. This indicated that the perceived barrier is not an important factor for Malaysian health professionals to comply with ISPs related with HIS uses, regardless of whether they have a long working experience or less in the healthcare sector. Meanwhile, Perceived Benefit of security-countermeasure and Trust significantly affect users' compliance behaviour towards HIS security policies in both groups. This indicates that if HIS users are aware of the benefit of security-countermeasure, which is able to prevent security threat, they are more likely to comply with ISPs. The current results are consistent with those reported in previous studies (Hovav & D'Arcy, 2012; Hagen et al., 2008). Meanwhile, Trust is shown to be one of the important factors for employees to comply and practise security behaviour adequately. Thus, management should document the ISPs efficiently, whereby the documents can be easily understood and applied by all employees in the organisation. On the other hand, Perceived Severity is only significant in users with low experience. The result shows that as new employees, they prefer to avoid any problem with the management of the hospital because of their carelessness in practising information security behaviour since they are trying to build their career in the organisation. Previous studies suggest that if employees perceive higher levels of penalties for non-compliance with ISPs such as loss of job or heavy fines, their non-compliance behaviour is likely to decrease (Siponen et al., 2010; Herath & Rao, 2009).

Even though some studies discussed above are significant and some are not, the current findings revealed that there are no statistical differences in the standard path between both groups.

Based on multi-group analysis results, both groups have a different perspective on Management Support concerning compliance behaviour of HIS security policies. The comparison between these groups shows that Management Support is very significant in influencing users with low experience, while the Management Support is not significant among highly experienced users. Most users with low eperience focus on building their reputation; hence, they are more careful and try to avoid any problems with the management. Moreover, new users will probably be sent for security training organised by the institutions. This will help them to be aware of any new policies related to HIS that have been implemented in the health institutions. In line with previous studies, Management Support was found to be important in promoting information security awareness among IS users (Al-Omari et al., 2012; Warkentin et al., 2011; Brady, 2010).

Moreover, the comparison between these groups showed that Perceived Susceptibility significantly influenced users' compliance behaviour toward HIS policies in the highly experienced group and the path was stronger than users with low experience. This indicates that highly experienced users are more aware of the importance of complying with HIS policies to prevent information security threats that can pose serious problems to the health institutions. Authors of previous studies also reported that experienced users who had experience with security incidents were more likely to comply with security policies (Bulgurcu et al., 2009).

As a conclusion, it is crucial to note the point that high HIS users have the capacity of absorbing the intellectual capacity and matured skills to deal with the growing levels of technological solutions to overcome the loss of health data. Moderate levels of agreements (40 to 59 percent) on the elements of managerial support in terms of information system security training deal with low HIS users. This is because new and less experienced health professionals may need the non-technical explanations on the mechanism of security tools for them to understand and comprehend the internal and external features of system on a regular basis. It will take a longer time for new users to catch up with the internal security infrastructure.

Lack of technical support may inspire system abuse through unintentional behaviour among HIS users and this may generate lower possibility of data protection within the health system. The results of PLS-SEM have visualized the need for supporting role of managers in speeding up the level of system catch up among low HIS users. The coefficient of determination (R-square) determines the explanatory power of the two models. It is observed that there are slight differences between R-squares of two models in which 63 percent of variations in compliance behaviour deal with high experience of HIS users, whereas 60 percent is tied up with low experience of HIS users. It has only supported two of the five formulated hypotheses. Lack of support for the remaining three hypotheses are due to the fact that low and high experiences of HIS users might have perceived similar levels of importance to the identifications of benefits within the actions, and trust to comply with the security policies. Besides that, matured technical skills among highly experienced health professionals will be able to guide them to catch up with the innovative nature of protective security tools to prevent loss of data or damages. The records of diseases and precautionary medications should be maintained carefully in order for them to take care of long term health care.

4.6.3 Linking the Quantitative and Qualitative Phases through Prototype Development and Testing

Figure 4.6 shows the linking process of the quantitative phase and qualitative phase. The quantitative phase of this study has provided useful findings for RQ2, which aimed at gauging the direct and indirect effect of HISSPC factors, and affirmed that most of the factors significantly affected health professionals' compliance behaviour towards HIS security policies. The quantitative research findings are important to the practitioner as they show that the prescribed dimensions incorporated into a prototype design might increase the compliance behaviour towards ISPs among HIS users. Therefore, they provide the empirical justification of the usefulness of the HISSPC Model as validated by the real users during prototype testing.

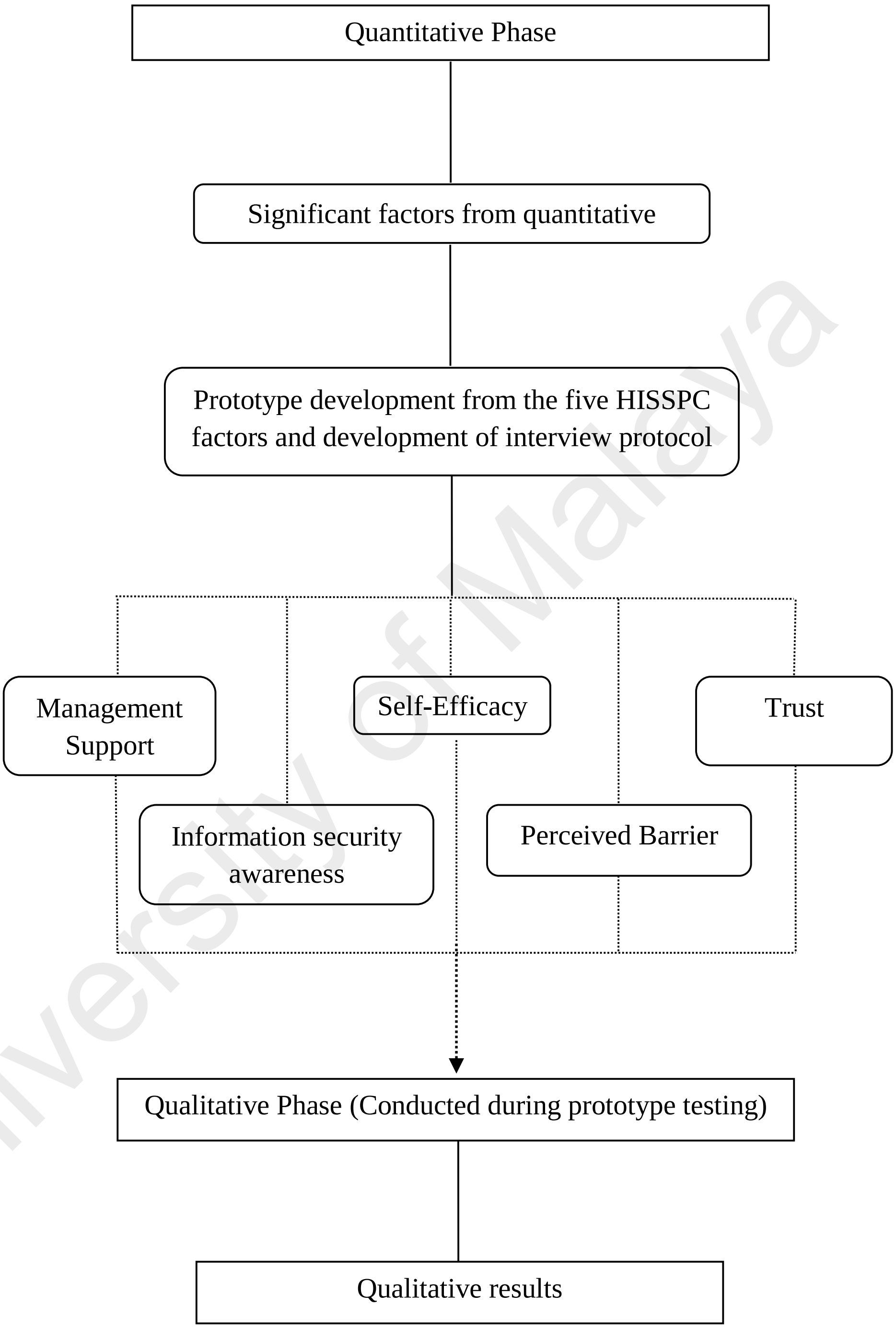

Quantitative Phase
Significant factors from quantitative
Prototype development from the five HISSPC factors and development of interview protocol
Management Support
Self-Efficacy
Trust
Information security awareness
Perceived Barrier
Qualitative Phase (Conducted during prototype testing)
Qualitative results

Figure 4.6: Linking quantitative phase and qualitative phase. (The dotted lines represent the integration of quantitative phase and qualitative phase.)

The HIS prototype was designed using Unified Modelling Language (UML) and developed using several software development tools, which is explained in Chapter Five. Additionally, the HIS prototype was developed with the aim to manage information security policy announcements or notifications to all employees in the health institution effectively and systematically based on the significant factors in the HISSPC Model. In order to ensure that the prototype was useful in improving the users' compliance behaviour towards ISPs, the qualitative research technique was chosen as it is believed to increase our understanding and to obtain a more holistic picture concerning the compliance behaviour issue towards HIS security policies in health institutions.

The goal of the qualitative phase inside the prototype testing phase in the current research was to examine users' perception about the proposed HIS prototype, which helped to clarify the results in the quantitative phase in more depth. Further, the current study explored areas potentially related to the enhancement of health professionals' compliance behaviour towards HIS security policies through HIS prototype. Thus, the design of the interview protocol focused on obtaining a more holistic picture of how health professionals or HIS users comply with ISPs related to HIS use.

CHAPTER 5: DESIGN AND IMPLEMENTATION OF THE PROTOTYPE

5.1 Introduction

This chapter explains the prototype development methodology, prototype architecture, and prototype module interfaces that have been designed to develop the HIS prototype. In addition, the chapter also covers the hardware and the software used in the development of the Health Information System (HIS) prototype.

In the current study, the Waterfall Model was adapted as the prototype implementation methodology, whereby the details of the prototype's functionalities and its structures are described using the Unified Modeling Languages (UML), through which the Use Case view and logical view of the prototype are modeled.

5.2 PLS-SEM Analysis

The requirements of the prototype modules were identified based on the PLS-SEM analysis discussed in the previous chapter, and the prototype was developed to achieve research question 3, which was to evaluate the usefulness of the HISSPC model with the aim to improve the compliance behaviour of health professionals towards HIS security policies. The PLS-SEM analysis found that the management support influenced the health professionals' information security awareness and compliance behaviour towards HIS security policies. Moreover, Information Security Awareness (Perceived benefit and Perceived severity), Self-efficacy, Perceived barrier, and Perceived trust also influenced the health professionals' information security compliance behaviour towards HIS security policies.

5.2.1 User Identification

As discussed in chapter three, this study only focused on health professionals who are the HIS users. Health professionals are the doctors, supporting staff (nurses, pharmacists, radiologists, among others), and health administrators. The management of health institutions that manage HIS are the Information Technology (IT) staff. Therefore, the IT staffs are responsible for handling the HIS configuration and create new announcements of HIS security policies and information security threats to be distributed to all HIS users through the hospital internal website.

The development of the HIS prototype in this study focused on the factors that influenced users' compliance behaviour towards HIS security policies that were implemented in the health institutions with the aim to improve information security behaviour among health professionals. The prototype requirements for each user are described in the next section.

5.2.2 Prototype Requirements

The prototype requirements were prepared according to the users' needs, in relation to the factors that influenced the users' compliance behaviour with the HIS security policies. These requirements were determined based on the analysis on the current system and the survey analysis using the PLS-SEM, which focused on several significant factors – Management support, Information Security Awareness, Self-Efficacy, Perceived Barrier, and Perceived Trust – as shown in Table 5.1.

Table 5.1: The significant factors and HIS prototype modules

Significant Factors	Prototype Modules	Current HIS
Management Support	Manage HIS users.	Current system use internal email to alert and distribute HIS security policies.
	Manage for users to receive and read online announcement messages and notifications.	
	Manage any information updated related to HIS security policies, information security threats and HIS training.	
	Manage HIS Short Message System (SMS) configuration.	
Information Security Awareness (measured based on three factors: Perceived Benefit, Perceived Severity and Perceived Susceptibility	Receive online announcement messages and SMS notification: • ISPs announcements • Information security threat alerts	Not available in current HIS.
	Receive notofications through SMS systems.	
Self-Efficacy	• E-training	Not available in current HIS. The training was conducted manually.
Perceived Barrier	No specific module develops for these factors. Basically, HIS users were interviewed to get their perceptions towards the proposed system such as in terms of the difficulty of using the proposed prototype and their confidence level.	
Trust		

Below are the details of the module requirements for each user:

5.2.2.1 Information Technology (IT) Administrator

The HIS modules are implemented for the IT administrator to show that the hospital management is concerned about the information security issues, which supported the behaviour of practicing information security in daily works. These modules are explained below:

a) Manage HIS Users

The IT administrator is responsible to manage the HIS user information, as stated below:

- Register new users

  New users are registered by an IT administrator, once the health institution employs a new employee. Several data related to the employee are stored in the database. However, this study only focused on a few data for the purpose of distributing HIS security policies announcements and notifications. The data required to register the users in this prototype are the users' ID, password, display name, email, and phone number.

- Update, Delete, and View users

  The IT administrator is authorised to update or delete any user data that is currently stored in the database, if needed. Other than that, the IT administrator can also monitor users' behaviour via viewing and reading the announcements or notifications about HIS security policies or updated information security threats that are distributed using pop up messages in the hospital internal website.

The module can help the management to control and monitor their employees by ensuring that all the employees receive the announcements or notifications about HIS security policies updated by the IT administrator.

b) Manage any information updated related to HIS security policies, information security threat and HIS training.

The IT administrator is responsible for managing any information updates related to HIS security policies, information security threats and HIS training, such as creating, updating, and deleting online announcement messages and notifications. This is where the management shows their support towards information security.

If the management implements any new security policy related to the HIS uses, the IT administrator is responsible to ensure that all HIS users get the current information of ISPs and information security threats.

c) Manage HIS SMS configuration

The IT administrator is responsible for inserting or updating SMS configuration information that is used to alert HIS users about any news related to HIS security policies announcements and notifications through mobile devices.

5.2.2.2 Health Professionals

The HIS modules designed for the health professionals are stated below:

a) Receive Online Announcement Messages

Any new or updated security policies related to HIS uses are notified to the HIS users through the HIS internal website. The HIS security policies announcement pops up when the HIS users log in to the system.

This module is believed to increase the users' awareness concerning any new policies related to the HIS that is implemented in the hospital, and any information related to information security threats that currently exist. It is also believed that if users' information security awareness is increased, then, security incidents can be decreased. Furthermore, the online HIS security policies announcements and notifications can develop both the users' Self-Efficacy and Trust towards the organization's information security policies (ISPs) . Users get the information in the form of texts, audio or video, which helps improve their knowledge. In addition, the barriers to using information security technology are also reduced as the users' knowledge increases.

b) Notifications through the Short Message Service (SMS) system

The SMS system aims to alert the users about any new online information security announcement that is distributed by the management. Thus, the users will check the message when they log in to the hospital internal system. This system will increase user's information security awareness.

5.2.3 Prototype Behaviour

The prototype behaviour is identified using the Use Cases Model and the Use Cases relationship between the users. In the Use Cases Model, the users are normally called actors. The relationship between the actors and the use cases are explained as follows:

5.2.3.1 Use Case Diagram for Health Professionals

Figure 5.1 shows the Use Cases Model for health professionals that illustrates the system's functions, its surroundings, and the relationships between the actors and the use cases. Each use case begins when the system verifies authorized users. Therefore, users or actors need to have user IDs and passwords before accessing the system.

There are two use cases associated with the health professionals that are focused upon in this study – login and receiving online announcement messages or notifications.

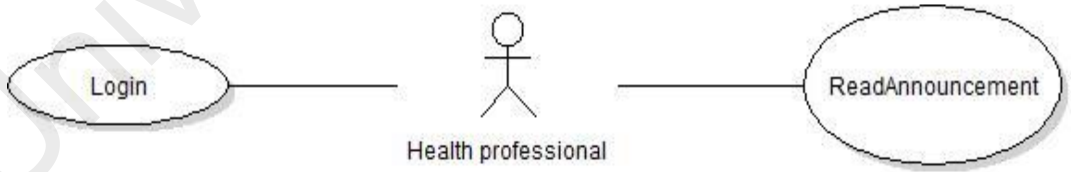


Figure 5.1: Use case associated to health professional

5.2.3.2 Use Case Diagram for IT Administrator

Figure 5.2 shows the Use Cases Model for IT administrators that illustrates the system's functions, its surroundings, and the relationships between the actors and use cases. Each use case begins when the system verifies the authorized users. Therefore, the IT administrator or the actors need to have user IDs and passwords before accessing the system.

There are nine use cases that are associated with the IT administrator. The use cases that are focused on in this study are login, create/update/delete HIS security policies announcement messages or notifications, register/update/delete/view users, and manage SMS configuration for HIS.

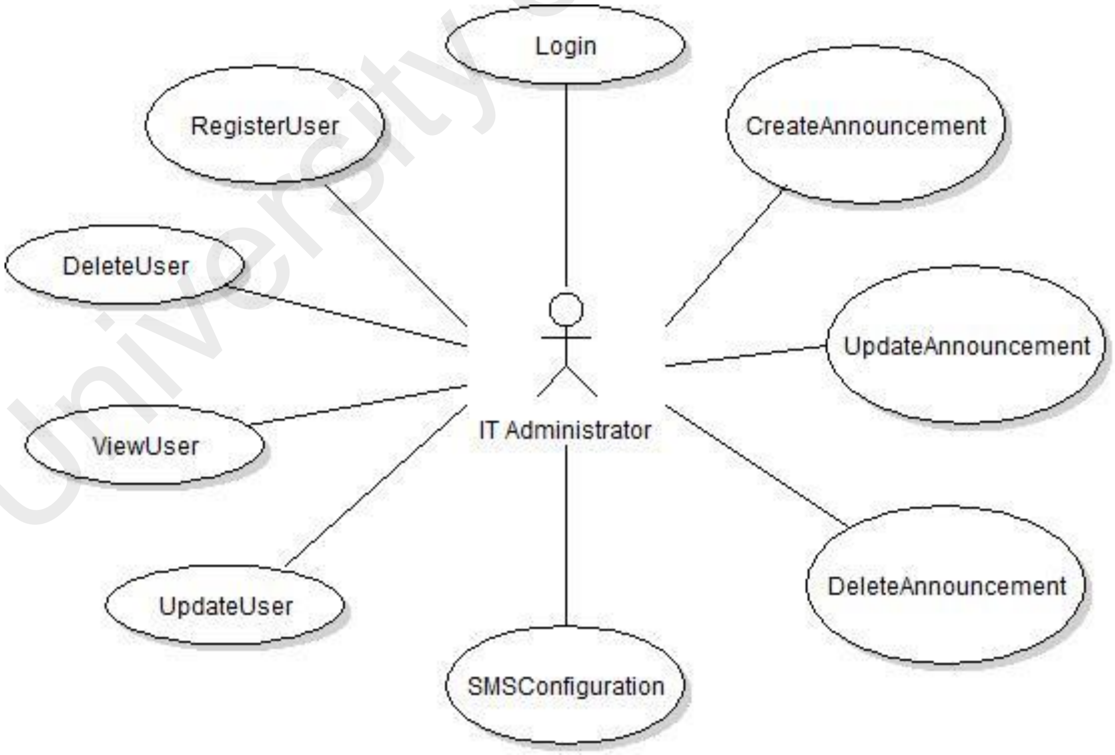


Figure 5.2: Use case associated to IT Administrator

5.2.4 Sequence Diagram

Use case realisation is represented using a sequence diagram that includes a description of the classes that are involved in carrying out each individual use case. It also involves the description of the different types of interaction between the use case elements. However, this chapter only focuses on the main use case that maps the significant factors, as stated earlier.

5.2.4.1 Sequence Diagram of Use Cases for Health Professionals

The sequence diagram for the use case for health professional actors is illustrated below.

a) Receiving online announcement message and notification of events

After the system verifies the users' authentication and view status, they will automatically receive a pop up message that contains information about HIS security policies, HIS training or any news regarding current information security threat. This pop up message, known as information security announcements or notifications, is retrieved from the announcement file in the database, as illustrated in Figure 5.3. If the users have already viewed and read the announcements or notification messages, the users will not receive a further pop up message when they log in to the system for the second time, unless a later announcement or notification is created and distributed by the IT administrator.

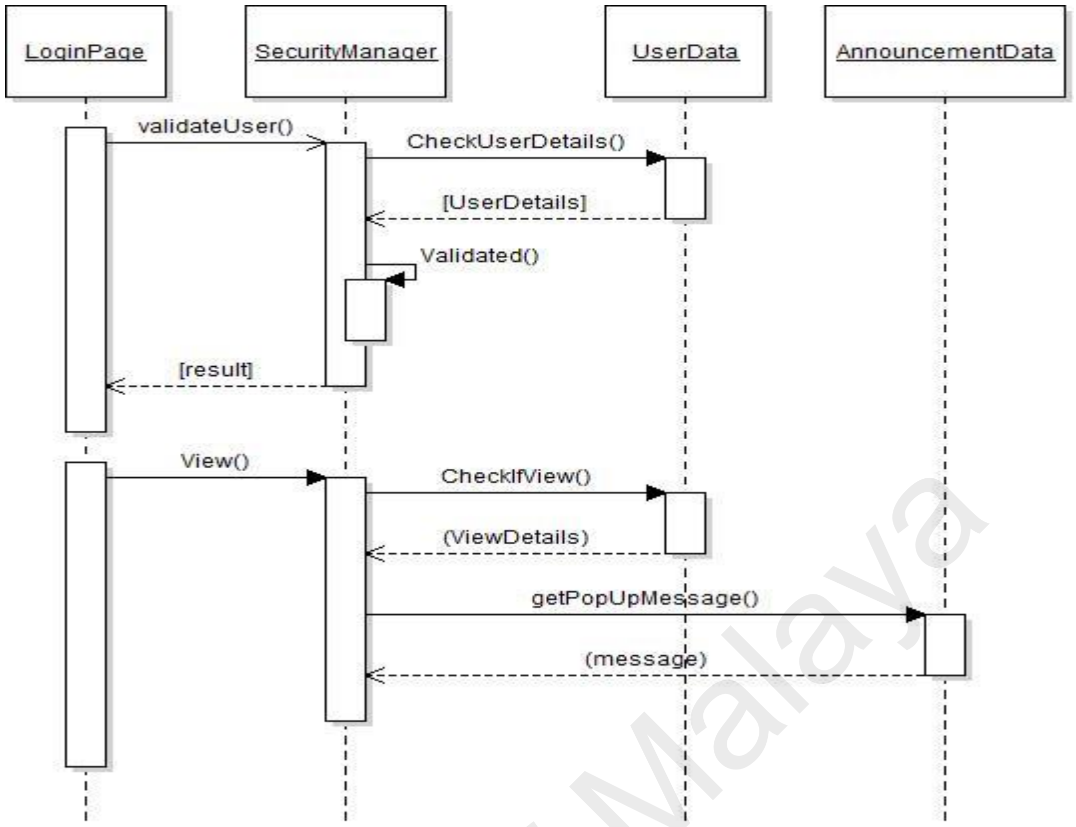


Figure 5.3: Sequence diagram of the use case to read HIS security policies online announcement and notification

5.2.4.2 Sequence Diagram of Use Cases for IT Administrator

The sequence diagrams of use case for the IT administrator are illustrated below.

a) View user login details event

The IT administrator can view users' details that are retrieved from the database. The data are displayed on the user table interface, as illustrated in Figure 5.4. This function can allow the IT administrator to monitor if the users have received and read the online announcement messages or notifications that are currently posted.

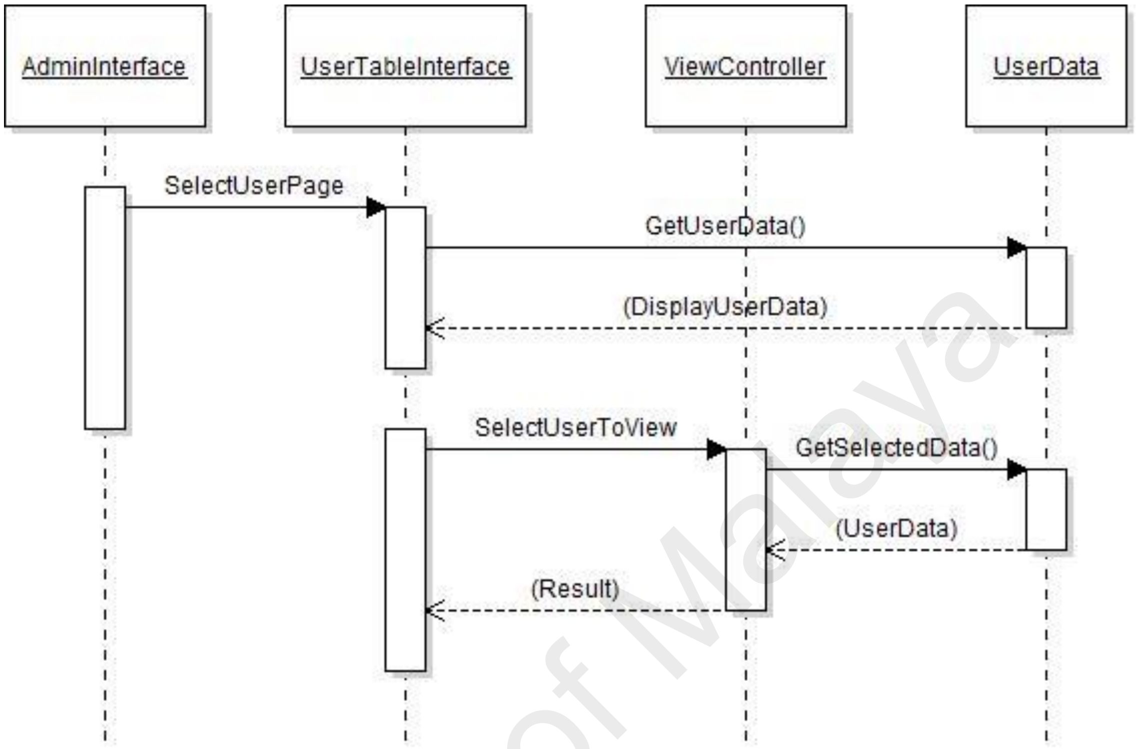


Figure 5.4: Sequence diagram of the use case view user details event

b) Create online announcement or notification events

The IT administrator is responsible for creating and posting online announcement messages or notifications related to HIS security policies, training and information security threats. In doing so, the IT administrator must select the announcement form interface and insert any data required to be displayed in the announcement or notification message. The data required in this event are announcement title and announcement content. Announcement or notification contents can be text or video, or both.

After the announcements or notifications are created, the system retrieves the users' phone numbers for the purpose of SMS notification. The SMS configuration command is executed to invoke the SMS system. This is illustrated in Figure 5.5.

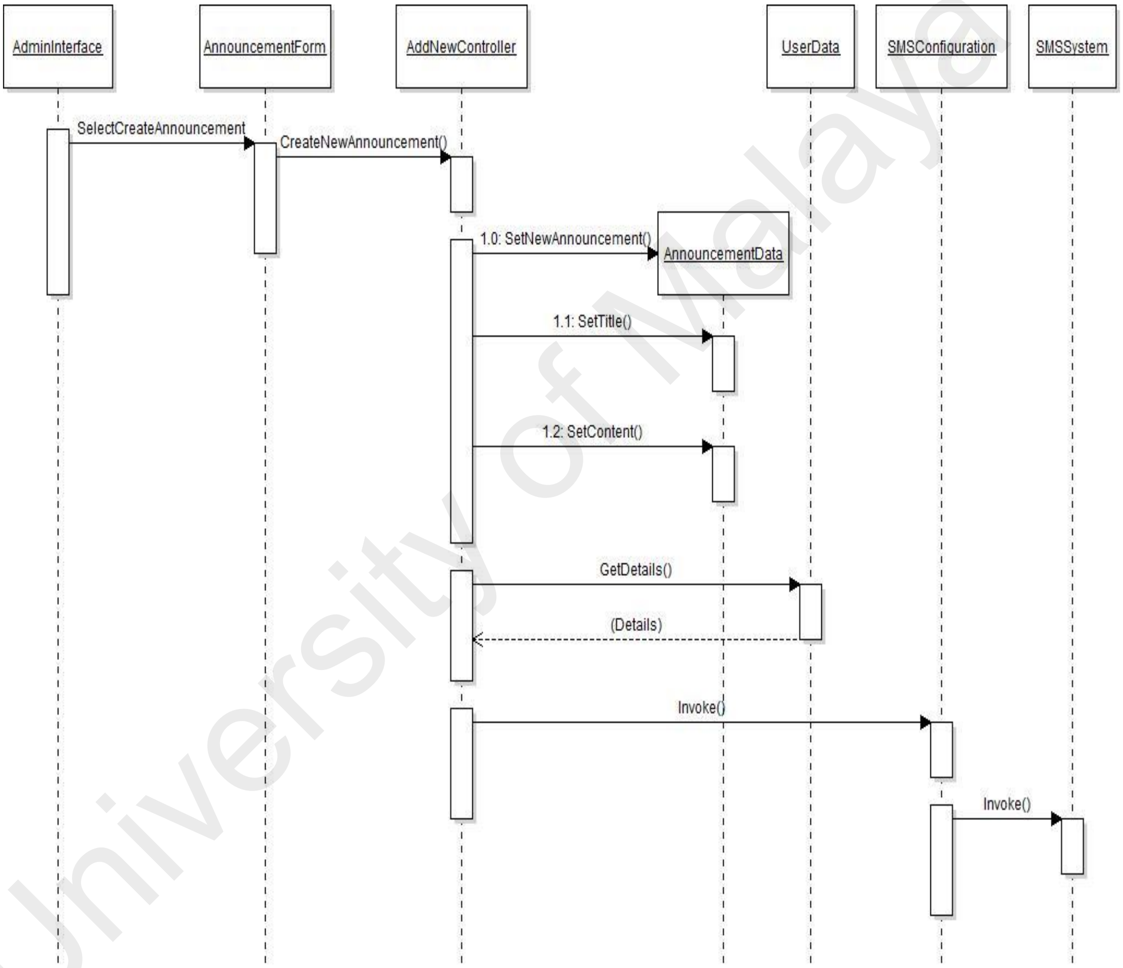


Figure 5.5: Sequence diagram of the use case to create online announcement and notification events

c) Update online announcement and notification events

The IT administrator is allowed to update any current announcement or notification. In doing so, the IT administrator must select the current announcement interface and select any new announcement to be updated.

The users' phone numbers are retrieved from the database, and the SMS configuration command is executed to invoke the SMS system. This is illustrated in Figure 5.6.

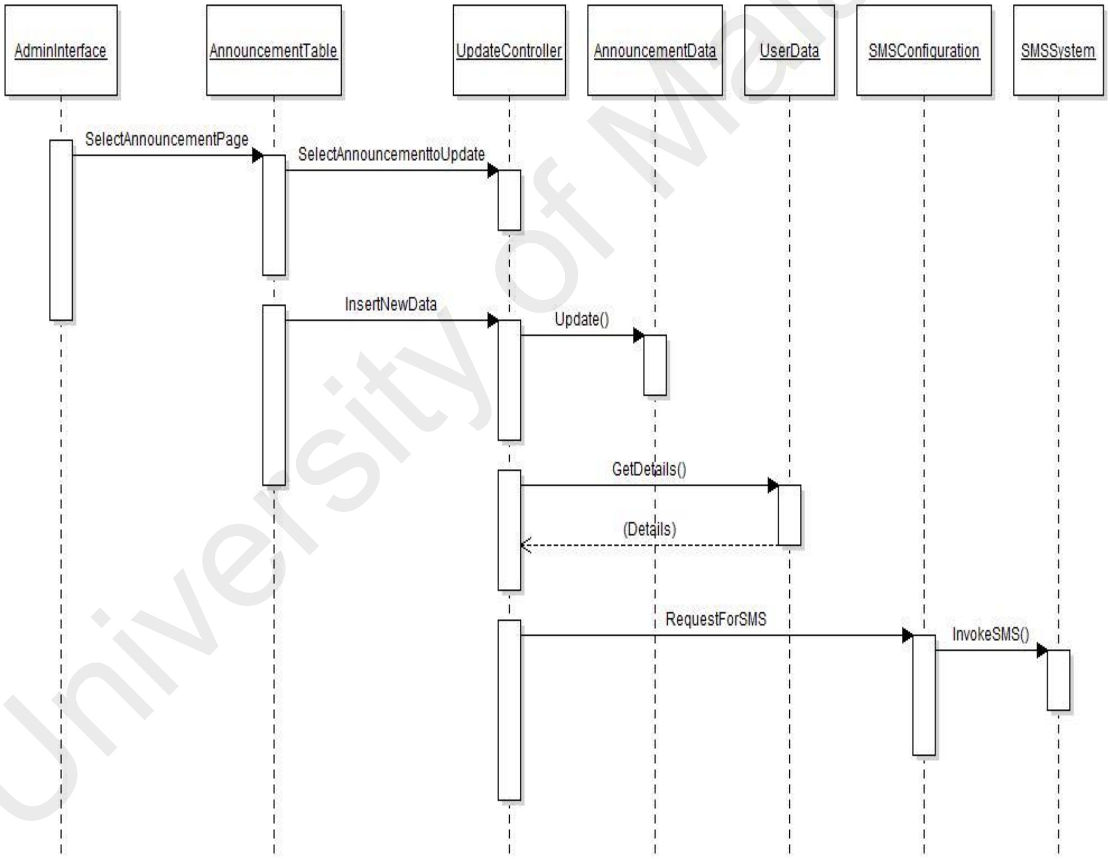


Figure 5.6: Sequence diagram of the use case to update online announcement and notification events

d) Delete online announcement and notification events

The IT administrator is allowed to delete any announcement or notification that is no longer required in the database. In doing so, the IT administrator must select a current announcement interface and select any existing announcement or notification that they wish to delete. Then, the system sends a delete notification message to be acknowledged by the IT administrator. If the yes notification is chosen, the announcement data are deleted automatically from the database, as illustrated in Figure 5.7.

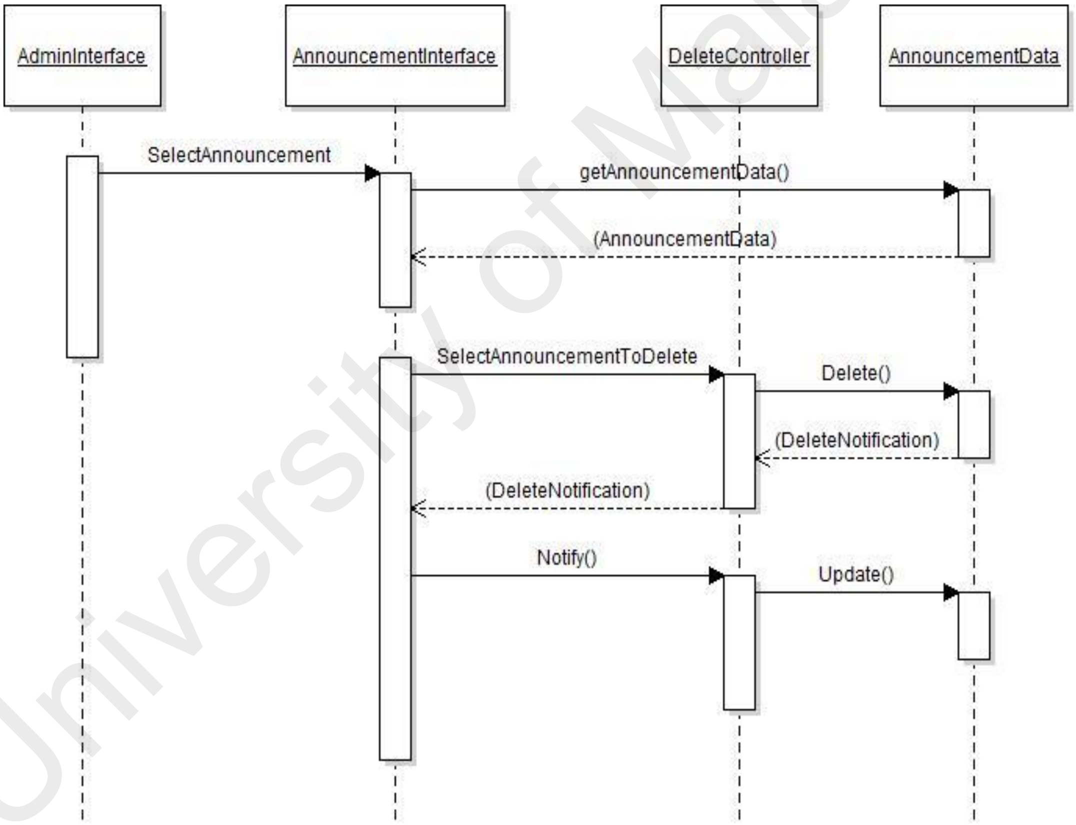


Figure 5.7: Sequence diagram of the use case to delete online announcement and notification events

e) Managing HIS SMS configuration

The IT administrator is responsible for managing the SMS configuration information. After the login succeeds, the IT administrator selects the configuration interface and goes to the Twilio system configuration form interface. The data required for the Twilio SMS configuration are Twilio SMS number, Twilio account identification number (ID), and Twilio account token. The data entry is verified by the configuration controller to avoid any data error before sending the data to the SMS configuration file in the database system. This is illustrated in Figure 5.8.

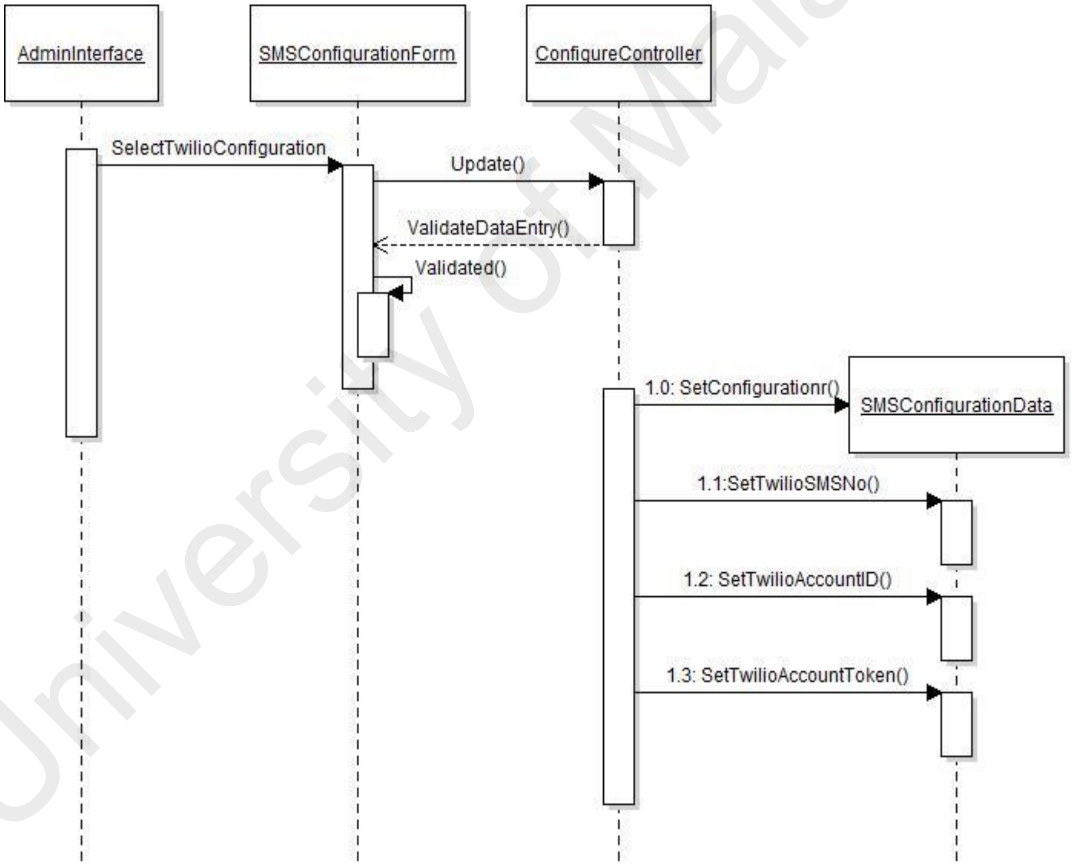


Figure 5.8: Sequence diagram of the use case to manage HIS SMS configuration

5.2.5 Class Diagram

This section presents the structures that comprise the skeleton of the HIS prototype that is modeled. The class diagram acts as a data dictionary that describes all the possible data structures and relationships that control the input and output of the data system.

The UML class diagram is used to describe the classes involved in realising the functionalities of the prototype, as shown in Figure 5.9. The diagram also shows the interrelationships between the candidate classes. The candidate classes for the purpose of the prototype are user file, HIS security policies announcement file, admin file, and the SMS configuration file, while the SMS is handled by the Twilio SMS system.

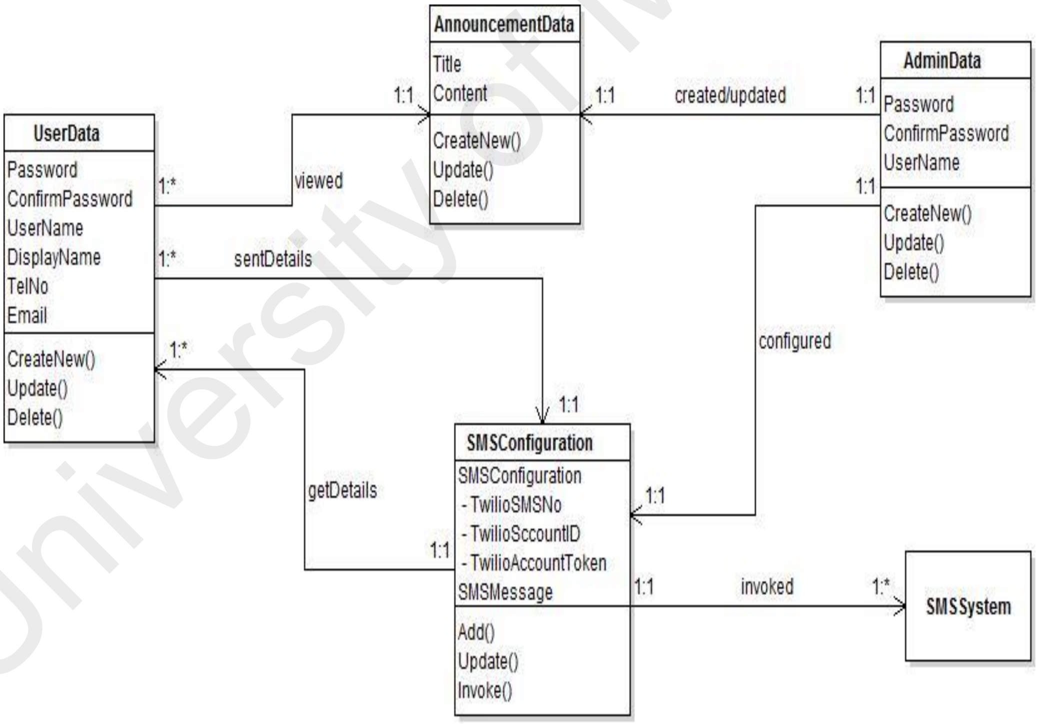


Figure 5.9: Class diagram

5.3 Hardware Requirement

The hardware that was required for the setting up of the HIS prototype included a compatible PC, which acted as a server and connected to the clients' computers via the network. The clients' computers could be PCs, Laptops, workstations or any devices that are installed with an Internet browser, such as Internet Explorer, Netscape, or Mozilla. The server configuration system is Linux Apache version HTTPD 2.2.26 (Win32). This system has the responsibility for establishing the connection between the clients and the server, processing the clients' requests, delivering data to the clients, controlling the communication between the clients and the server, and, finally, displaying the status and the results of a user's query.

5.4 Software Requirement

Several software development tools were used in the system development. The tools were divided into four categories – server management tools, database tools, application tools, and programming tools.

a) Server Tool

The server used is Linux Apache HTTPD version 2.2.26 (win32).

b) Database Tool

MySQL version 5.1 was used to create the database system. This database application is named as PHPMyAdmin. The PHPMyAdmin has several functions for the administrator to manage the entire data store in the database. By using this tool, the database administrator can create new databases, tables, and fields that were required for the system.

c) Application Tool

Various techniques and tools were used in the system application interface design to design the main page and the internal pages. The application tool used to design the main page interface was Wordpress version 3.6, while the application tool to design the internal site pages was UserCake version 2.0.2. These application tools provide system navigation, graphics, applets, programming, and other applications. These application tools are able to provide an attractive interface with a combination of creativity and colour selection. Designing the system template is also easy with the use of these application tools.

d) Programming Tool

PHP scripting language version 5.3 was used for the programming or logical design of the system. This programming language can create dynamic pages and connect to the database system.

5.5 System Architecture

The system architecture consists of the server, user desktop or any user workstation, SMS alert notification system, and mobile phone device, as shown in Figure 5.10.

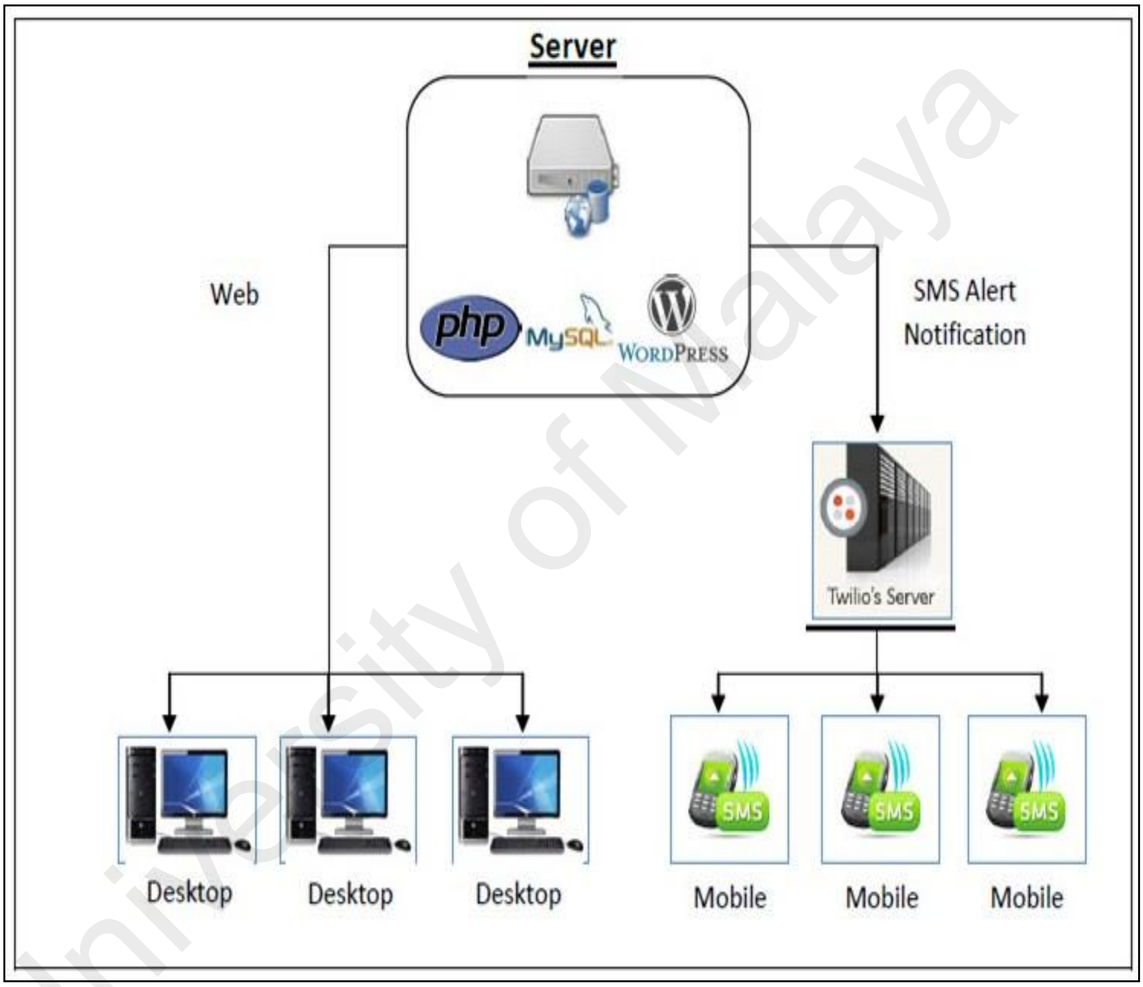


Figure 5.10: HIS prototype architecture

a) Server

The server was hosted online. The portal was developed in the Wordpress Content Management System (CMS).

b) Twilio

SMS service from the Twilio SMS service was used to invoke the SMS system. The account for the SMS service was registered on this website (http://www.twilio.com). The Twilio SMS service charged every SMS at USD0.01.

c) Desktop

Clients can access the application via their browser since it is a web-based application. Any updates regarding the ISPs related to HIS are seen in the pop up window in the internal hospital system, once the user logs in.

d) Mobile

The users' mobile phones will receive SMS notifications from the Twilio, once the IT administrator posts online ISPs announcements or notifications regarding any new updates of the HIS security policies or information security threats.

5.6 Prototype Module Interfaces

Nine module interfaces were designed to develop the HIS prototype, as described in the following section. The nine module interfaces were designed based on the users' requirements discussed in the previous section. However, in this study, the researcher only discusses the main modules of the HIS prototype.

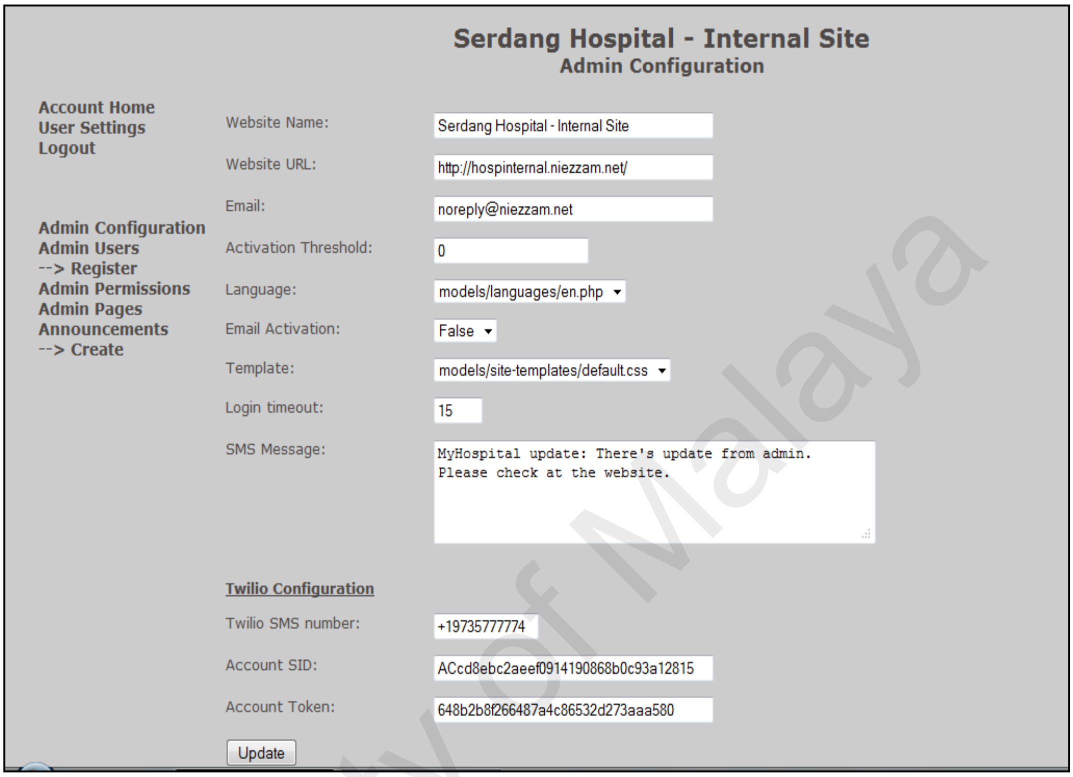
5.6.1 Administrator Modules

The main module used by the IT administrator consists of an SMS configuration interface, user information table interface, create online announcement interface, and online announcement table interface.

a) Configuration Interface

The SMS configuration interface is designed for the IT administrator to configure the website information and SMS information, as shown in Figure 5.11. The IT administrator is allowed to update any changes about the website and SMS configurations. In the website configuration form, the IT administrator is required to insert information related to the hospital website, such as website name and website Uniform Resource Locator (URL).

Other than that, the IT administrator can control the user's login by inserting the period of login timeout. The purpose of login timeout is to ensure that a user's computer is logged out if the computer is in idle mode for a certain period that is set up by the IT administrator. This function is proposed to avoid any unauthorized access and to protect the system from internal threats.



Serdang Hospital - Internal Site
Admin Configuration

Website Name: Serdang Hospital - Internal Site

Website URL: http://hospinternal.niezzam.net/

Email: noreply@niezzam.net

Activation Threshold: 0

Language: models/languages/en.php

Email Activation: False

Template: models/site-templates/default.css

Login timeout: 15

SMS Message:

```
MyHospital update: There's update from admin.
Please check at the website.
```

Twilio Configuration

Twilio SMS number: +19735777774

Account SID: ACcd8ebc2aeef0914190868b0c93a12815

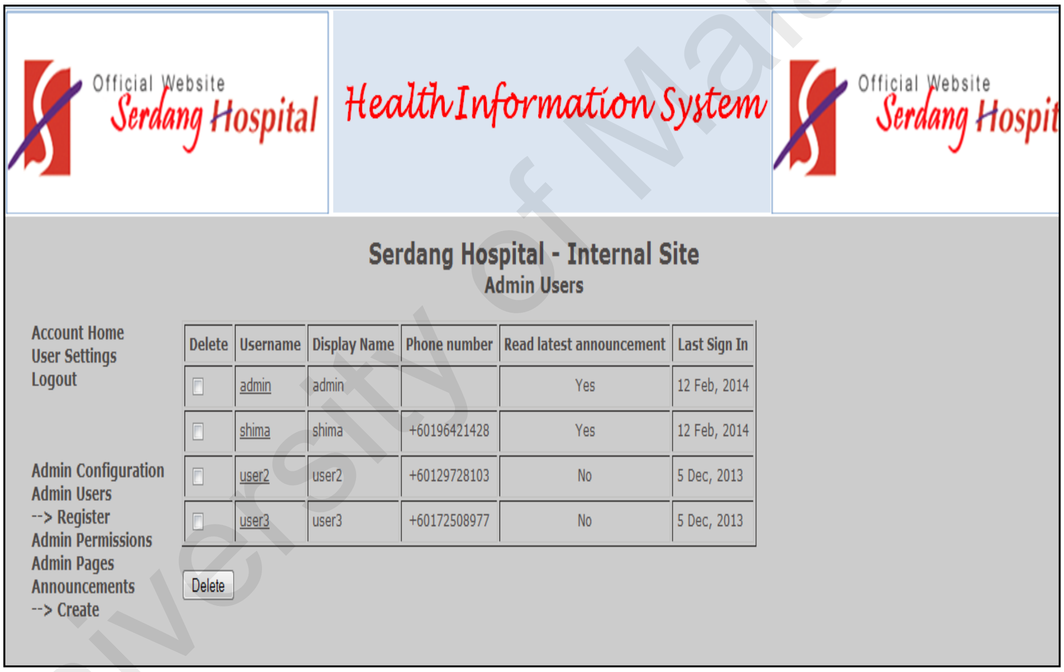
Account Token: 648b2b8f266487a4c86532d273aaa580

Figure 5.11: SMS configuration interface

b) User’s Information Table Interface

The IT administrator can retrieve a user’s data from the user’s file in the database. The information is displayed in the user’s table, which contains the username, display name, phone number, read latest announcement and the date of last entry into the system, as shown in Figure 5.12.

In this interface, the IT administrator can monitor a user's behaviour and if the user has received and read the posted online announcement messages or notifications. Apart from this, the IT administrator is also allowed to delete any users that are no longer working in the current health institution. Firstly, the IT administrator has to choose a user in the username list column, and then, tick on the option box in the delete column of the table. After that, the IT administrator needs to press the delete button on the bottom of the table. Finally, the selected user is deleted automatically from the database.



Serdang Hospital - Internal Site
Admin Users

Delete	Username	Display Name	Phone number	Read latest announcement	Last Sign In
☐	admin	admin		Yes	12 Feb, 2014
☐	shima	shima	+60196421428	Yes	12 Feb, 2014
☐	user2	user2	+60129728103	No	5 Dec, 2013
☐	user3	user3	+60172508977	No	5 Dec, 2013

Figure 5.12: User's information table interface

c) Create Online Announcement Interface

Figure 5.13 shows the screenshot of the online announcement form interface. This interface provides a form that allows the IT Administrator to create an online announcement or notification that is posted to the health professionals who are working in the health institution.

In this interface, the form contains two text fields – title text field and content area field. The title text field is for inserting the title of the announcement messages or notifications that will be posted to the users. Meanwhile, the content area field is used to insert the content of the announcement or notification. The content can be text, audio and video. Several text tools were used to create the announcement content. The text tools help the IT Administrator to arrange and structure the objects in the content area. The steps to create an online announcement message are shown in Table 5.2.

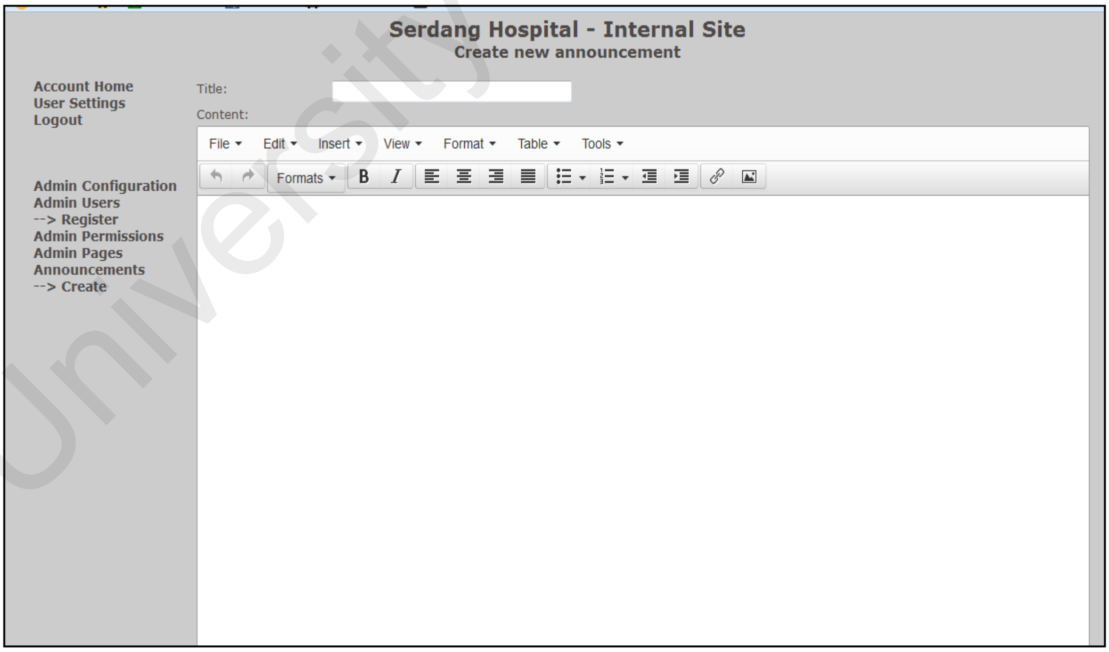
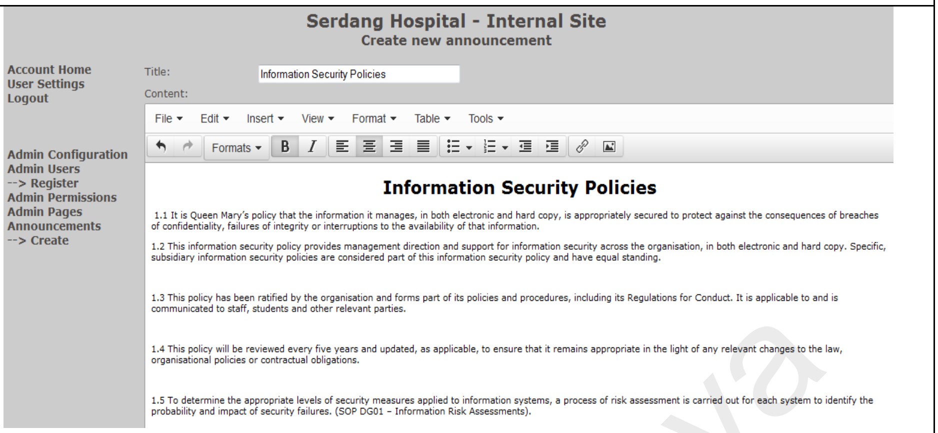
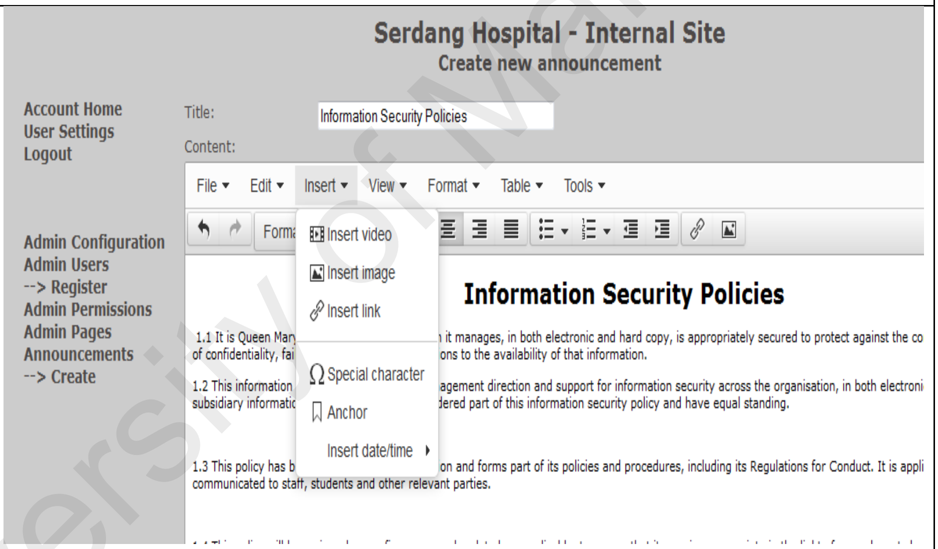
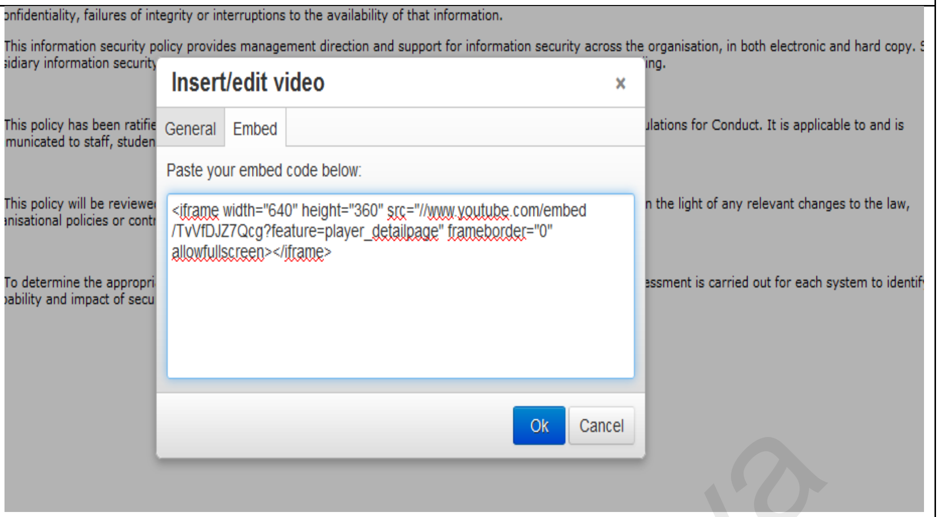
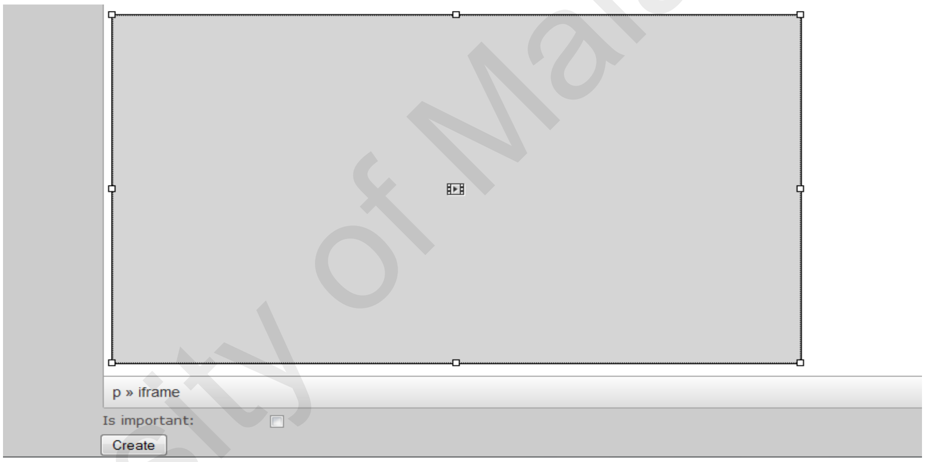


Figure 5.13: Online announcement interface

Table 5.2: Steps to create an online announcement message

Functions	Interfaces
Insert text	 Serdang Hospital - Internal Site Create new announcement Account Home User Settings Logout Admin Configuration Admin Users --> Register Admin Permissions Admin Pages Announcements --> Create File Edit Insert View Format Table Tools Formats Title: Information Security Policies Content: **Information Security Policies** 1.1 It is Queen Mary's policy that the information it manages, in both electronic and hard copy, is appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information. 1.2 This information security policy provides management direction and support for information security across the organisation, in both electronic and hard copy. Specific, subsidiary information security policies are considered part of this information security policy and have equal standing. 1.3 This policy has been ratified by the organisation and forms part of its policies and procedures, including its Regulations for Conduct. It is applicable to and is communicated to staff, students and other relevant parties. 1.4 This policy will be reviewed every five years and updated, as applicable, to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations. 1.5 To determine the appropriate levels of security measures applied to information systems, a process of risk assessment is carried out for each system to identify the probability and impact of security failures. (SOP DG01 – Information Risk Assessments). Figure 5.14: Insert text message
Insert video/image/link	 Serdang Hospital - Internal Site Create new announcement Account Home User Settings Logout Admin Configuration Admin Users --> Register Admin Permissions Admin Pages Announcements --> Create File Edit Insert View Format Table Tools Formi Insert video Insert image Insert link Special character Anchor Insert date/time Title: Information Security Policies Content: **Information Security Policies** 1.1 It is Queen Mar i it manages, in both electronic and hard copy, is appropriately secured to protect against the co of confidentiality, fai ons to the availability of that information. 1.2 This information agement direction and support for information security across the organisation, in both electroni subsidiary informatic dered part of this information security policy and have equal standing. 1.3 This policy has b on and forms part of its policies and procedures, including its Regulations for Conduct. It is appli communicated to staff, students and other relevant parties. Figure 5.15:Insert video message

Functions	Interfaces
	 Insert/edit video × General Embed Paste your embed code below: Ok Cancel `<iframe width="640" height="360" src="//www.youtube.com/embed/TvVfDJZ7Qcg?feature=player_detailpage" frameborder="0" allowfullscreen></iframe>` Figure 5.16: Embed video code  Figure 5.17: Create online announcement messages

There are several steps to create online announcement messages as following.

- In the content area field, IT administrators will insert text messages as shown in Figure 5.14.

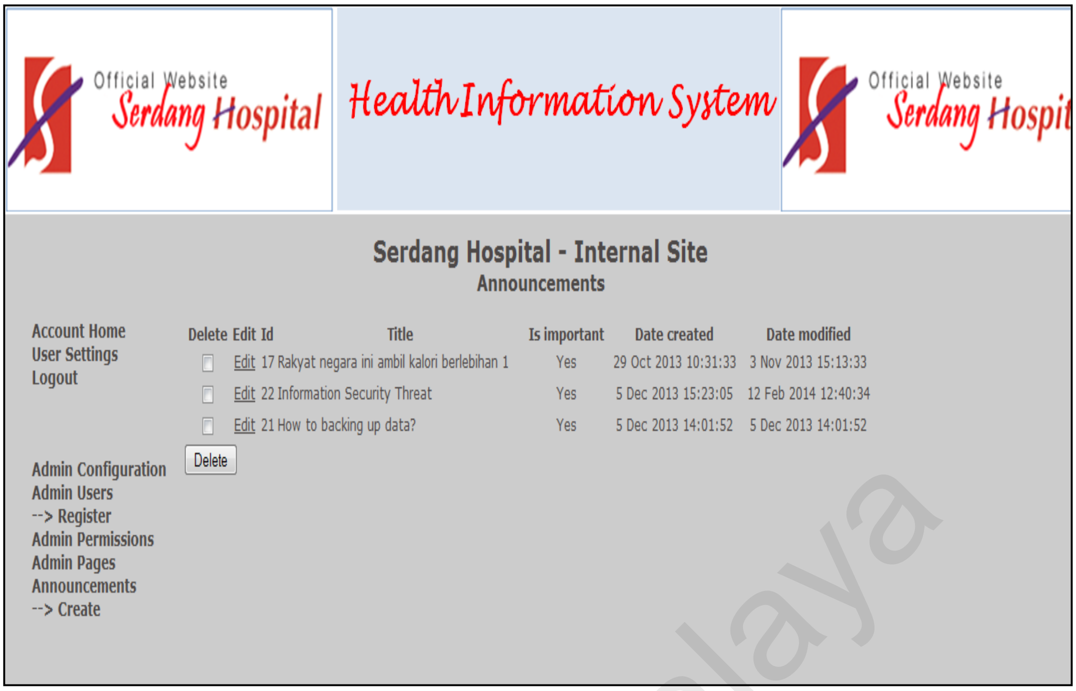
- If necessary, the video messages can also be inserted in the content area field by clicking *Insert pull down menu*, as shown in Figure 5.15. The *Insert pull down menu* contains several sub-menus, such as *Insert Video, Insert Image and Insert Links*. In this case, the *Insert Video sub-menu* was selected, and the insert/edit video interface will pop-up as shown in Figure 5.16. On this interface, the IT administrators will insert the code to display the required video.

- The IT administrators will click the *Create Button* to create the online announcement message and distribute to all users. If this message is important, the IT administrators need to click the *Is Important Check Box* before clicking *Create Button*, as shown in Figure 5.17.

d) Online Announcement Table Interface

Figure 5.18 shows the screenshot of the online announcement table interface. In this interface, the system retrieves the existing online announcement or notification that is created by the IT administrator. The information displayed in this interface is the announcement identification number, announcement title, important option, date created, and date modified.

In this interface, the IT administrator is allowed to perform two actions – edit/update and delete the existing announcement or notification. If the IT administrator wishes to edit/update the existing announcement or notification, he/she can click on the Edit hyperlink, and then the system will bring it to the Edit Online Announcement interface, as shown in Figure 5.19.

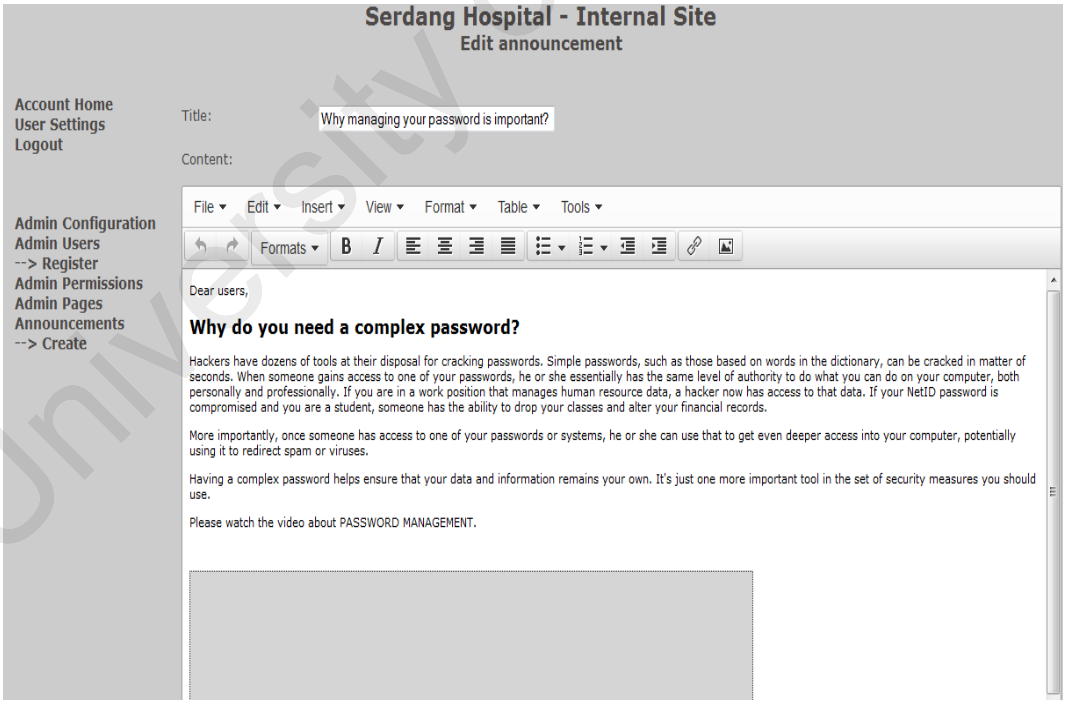


Serdang Hospital - Internal Site

Announcements

Delete	Edit	Id	Title	Is important	Date created	Date modified
□	Edit	17	Rakyat negara ini ambil kalori berlebihan 1	Yes	29 Oct 2013 10:31:33	3 Nov 2013 15:13:33
□	Edit	22	Information Security Threat	Yes	5 Dec 2013 15:23:05	12 Feb 2014 12:40:34
□	Edit	21	How to backing up data?	Yes	5 Dec 2013 14:01:52	5 Dec 2013 14:01:52

Figure 5.18: Online announcement table interface



Serdang Hospital - Internal Site

Edit announcement

Title: Why managing your password is important?

Content:

Dear users,

Why do you need a complex password?

Hackers have dozens of tools at their disposal for cracking passwords. Simple passwords, such as those based on words in the dictionary, can be cracked in matter of seconds. When someone gains access to one of your passwords, he or she essentially has the same level of authority to do what you can do on your computer, both personally and professionally. If you are in a work position that manages human resource data, a hacker now has access to that data. If your NetID password is compromised and you are a student, someone has the ability to drop your classes and alter your financial records.

More importantly, once someone has access to one of your passwords or systems, he or she can use that to get even deeper access into your computer, potentially using it to redirect spam or viruses.

Having a complex password helps ensure that your data and information remains your own. It's just one more important tool in the set of security measures you should use.

Please watch the video about PASSWORD MANAGEMENT.

Figure 5.19: Edit online announcement interface

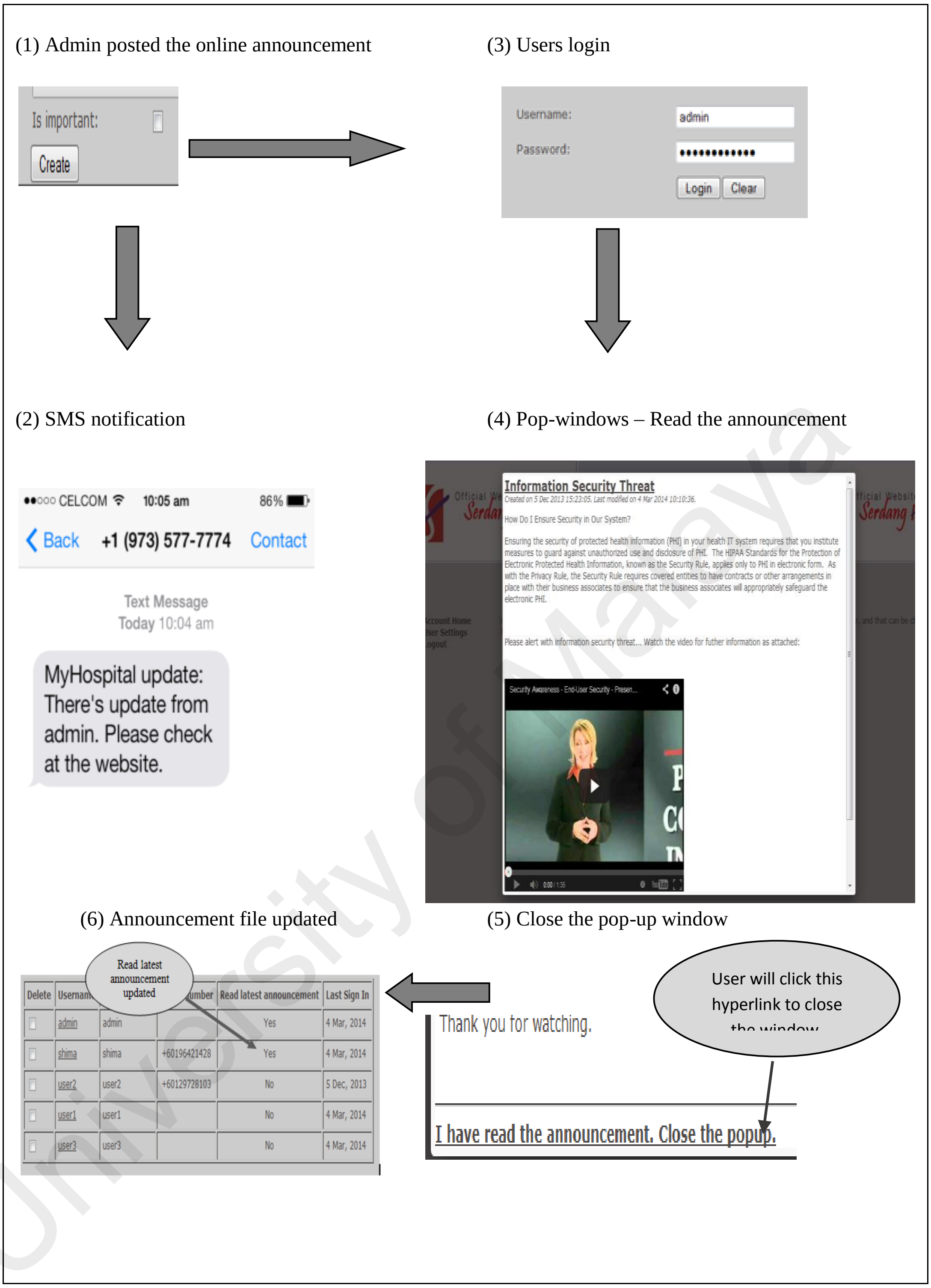
5.6.2 Health Professionals Modules

A module for health professionals was developed based on four factors: Information Security Awareness, Perceived Barrier, Self-Efficacy, and Perceived Trust. The purpose of this module is to announce or notify users about HIS security policies and any issues related to an information security threat in a faster way. The current practice that the management of the hospital applied to announce or notify users about HIS security policies or any issues regarding to the information security threat has been through the email system. However, this method is ineffective since many users do not read the email or just delete the email without reading the contents.

Therefore, the researcher believes that this module can help to increase users' knowledge towards HIS security policies and information security threats; thus, improving their information security awareness effectively. If users are aware of the severity of information security threat and the benefits of using security-countermeasure, then, users are likely to practice information security behaviour adequately, and compliant behaviour can be improved. Moreover, users' self-efficacy can be decreased, security barriers can be reduced, and users will be more confident with the HIS security policies that are implemented by Ministry of Health (MOH).

- Online Announcement or Notification Interface

The flow of users receiving an online announcement or notification is shown in Figure 5.20.



(1) Admin posted the online announcement

(2) SMS notification

MyHospital update: There's update from admin. Please check at the website.

(3) Users login

Username: admin

Password: ••••••••••••

(4) Pop-windows – Read the announcement

Information Security Threat

Created on 5 Dec 2013 15:23:05. Last modified on 4 Mar 2014 10:10:36.

How Do I Ensure Security in Our System?

Ensuring the security of protected health information (PHI) in your health IT system requires that you institute measures to guard against unauthorized use and disclosure of PHI. The HIPAA Standards for the Protection of Electronic Protected Health Information, known as the Security Rule, applies only to PHI in electronic form. As with the Privacy Rule, the Security Rule requires covered entities to have contracts or other arrangements in place with their business associates to ensure that the business associates will appropriately safeguard the electronic PHI.

Please alert with information security threat... Watch the video for futher information as attached:

(5) Close the pop-up window

Thank you for watching.

I have read the announcement. Close the popup.

(6) Announcement file updated

Delete	Usernam		umber	Read latest announcement	Last Sign In
□	admin	admin		Yes	4 Mar, 2014
□	shima	shima	+60196421428	Yes	4 Mar, 2014
□	user2	user2	+60129728103	No	5 Dec, 2013
□	user1	user1		No	4 Mar, 2014
□	user3	user3		No	4 Mar, 2014

Figure 5.20: Flow of posting and reading online announcement or notification

Referring to Figure 5.20, after the system verifies a user’s authentication and status, the online announcement or notification pop-up window interface will appear. The user can view and read the content of the announcements or notifications online before accessing the HIS sub-system. The pop-up window interface will be closed after the user presses the close button at the end of the page, and the system will update the user’s read status in the announcement file in the database to indicate that this particular user has already received the announcement or notification created by the IT administrator.

Other than that, the users also receive notifications through SMS. Moreover, any important announcements or notifications will be placed in the hospital website where health professionals can retrieve them at anytime and anywhere, when they need to refer to the information again.

CHAPTER 6: QUALITATIVE ANALYSIS, RESULTS & DISCUSSION

6.1 Introduction

Chapter 6 presents the results of the qualitative data analysis. The chapter begins with an explanation about the activities involved in prototype testing, followed by a description of the qualitative data analysis process, which covers the selection of the participants and the interviews that were conducted. The following section describes the findings of the qualitative research. Each of the research findings was interpreted according to the theme quoted during the coding process. The findings of the qualitative data were used to confirm the statistical evidence of the quantitative analysis of the current study. The qualitative data were analysed using Atlas.ti version 7.1. At the end of the chapter, the qualitative findings are discussed.

6.2 Prototype Testing

The prototype testing was carried out in two stages. In the first stage, the researcher ran system testing to test the system functionality. The system testing involved two modules: Information Technology (IT) administrator module and Health Information System (HIS) user module. The IT administrator module is a module to manage user information, online announcement/notification messages and SMS configuration, while the HIS user module is a module to retrieve online announcement/notification messages that are distributed by the IT Administrator. The results of the system testing showed that all the prototype modules were run successfully. The connection to the system was also successful without any problem.

In the second stage, the HIS user module was tested by HIS users to determine whether the proposed module is effective to improve users' compliance behaviour towards information security policies (ISPs) related with HIS uses. At this stage, the data was collected using the qualitative technique. The qualitative analysis and findings are discussed in the following section.

6.3 Qualitative Data Analysis

As mentioned in Chapter 3, qualitative data can reveal the "realism" aspect of investigating subjects. By using the interview approach, rather than retrieving answers based on fixed-option multiple choices, one is able to obtain data that are context-oriented and of interest, that is, compliance behaviour towards HIS security policies.

All the participants selected in the interview section were HIS users from different positions. This is because some employees may be more aware or sensitive to certain issues than other employees, as each of them holds a unique position that can influence their experience and perceptions. Table 6.1 presents the profiles of the interviewees for this study.

Table 6.1: Participant's profile

Demographic	Sungai Buloh Hospital	Serdang Hospital	Selayang Hospital	Total (n = 18)
Position				
Doctor	3	1	2	6
Support Staff	2	2	3	7
Health Record Administrator	0	2	3	5
Gender				
Male	1	1	1	3
Female	4	4	7	15
HIS Experience				
More than 5 years	1	2	4	7
Less than 5 years	4	3	4	11

The participants profile (Table 6.1) shows that there are five participants in the Sungai Buloh Hospital and Serdang Hospital group and eight in the Hospital Selayang group. The majority of the participants were support staff (nurses, pharmacists, radiologists, etc.) with the total number of n = 7, female (n = 15) and experience of using HIS for more than five years (n = 11). Each of the participants was interviewed via one-to-one interviews in the office at the particular hospital that the employee works for the purpose of tracking their perceptions towards the issue. Each interview lasted about 1 hour. By using an interpretive approach – assuming the interviewee's role, moving from the parts to the entire interview data, and identifying common patterns – the researcher was able to delineate certain dimensions. More importantly, the qualitative findings were able to confirm the relationships among factors in the Health Information System Security Policies Compliance (HISSPC) model and to further explain the users' compliance behaviour towards HIS security policies.

The interview notes were organized to illustrate the users' perceptions towards the implementation of HIS security policies and the factors that influence them to comply with the policies with regard to certain aspects: Management Support, Information

Security Awareness, barriers to complying with security policies, Self-Efficacy and Trust. These aspects represent the interviewees' honest thoughts about how the organization and human-technical factors influence their compliance behaviour towards HIS security policies.

The interviews in this study focus on research question three as stated below, but were intentionally open to future refinement. The main research question for qualitative research is as stated below:

RQ3: How can the prototype be used to improve users' compliance behaviour towards HIS security policies?

The first step of the interview was communicated to the interviewees together with the purpose of the study and the reasons why they were asked to participate. Additionally, they were provided information in accordance with the Institutional Review Board for the use of Human Subjects in research regarding the steps taken to assure confidentiality and protection. As mentioned in Chapter 3, the interviews were recorded on audio tape with the permission of the interviewees. Through these interviews, information was collected pertaining to events, incidents, processes and issues surrounding the implementation of HIS security policies. In the interviews, participants were encouraged to use their own terminology and discuss topics and issues that they saw as the most salient from their particular perspective.

In the first place, the interviews were carried out using the same questions in the same order. However, after conducting a few initial interviews, the questions were refined and other questions were added based on the response provided. The interview questions are included in Appendix A.2.

6.4 Theme Development

Each of the interviewees' responses was organized according to the selected hospital. The participant's information is listed in Table 6.2.

Table 6.2: Participant's Information

Participant Number (PNO)	**Position**	**Gender**	**Hospital**	**HIS Experience**
P1	Doctor	Female	Hospital Selayang	More than 5 years
P2	Health Administrator	Female	Hospital Selayang	5 years
P3	Health Administrator	Female	Hospital Selayang	5 years
P4	Health Administrator	Female	Hospital Selayang	Less than 5 years
P5	Nurse	Female	Hospital Selayang	More than 5 years
P6	Doctor	Male	Hospital Selayang	4 years
P7	Nurse	Female	Hospital Selayang	4 years
P8	Pharmacist	Female	Hospital Selayang	3 years
P9	Doctor	Male	Hospital Serdang	3 years
P10	Health Administrator	Female	Hospital Serdang	Less than 5 years
P11	Health Administrator	Female	Hospital Serdang	Less than 5 years
P12	Nurse	Female	Hospital Serdang	More than 10 years
P13	Pharmacist	Female	Hospital Serdang	More than 10 years

Participant Number (PNO)	Position	Gender	Hospital	HIS Experience
P14	Nurse	Female	Hospital Sungai Buloh	More than 10 years
P15	Nurse	Female	Hospital Sungai Buloh	4 years
P16	Doctor	Female	Hospital Sungai Buloh	Less than 5 years
P17	Doctor	Male	Hospital Sungai Buloh	More than 10 years
P18	Doctor	Female	Hospital Sungai Buloh	Less than 5 years

The interview data were coded during open coding. The open coding was conducted concurrently with an ongoing iterative process of the qualitative data analysis. The reason for this technique was to conceptualise categories that reflected the interview data, converging the codes into sub-theme and primary theme. The primary themes in this study refer to the significant factors of the quantitative study.

The theme development started with an initial conceptual work based on the results of the quantitative analysis. After the initial conceptual work, the interview data were analysed to determine the most logical codes (axial coding). Then, the highlighted codes were refined to ensure the reliability of the codes (selective coding). The links between the various codes were also determined by the purpose to develop more possible coding, create related categories (which would become sub-themes) and determine how the categories are related to one another (which would become the primary themes).

Data collection continued throughout this process to further refine the themes and sub-themes. The collection of themes and sub-themes was not only reviewed as independent parts of the whole, but also holistically. The relationships among the themes were conceptualised with the aim of recognising the relationships among the various sub-processes, which, together, represent an institutional story about the particular issue. Over time, this story, and the various individual themes began to produce an emergent theory. Subject matter experts (SMEs) then reviewed the qualitative analysis as a means of independent verification regarding the logic and theoretical structure of the themes, sub-themes, and the institutional story constructed.

Considerable effort was exerted to develop and maintain rigour throughout the data collection and analysis, especially in terms of qualitative trustworthiness. Maintaining rigour was accomplished by keeping accurate accounts of the research within research journals, including observational notes, personal insights into the conceptualization, and notes on the methodological decisions made.

6.5 Qualitative Results Findings and Interpretation

The sub-themes were developed through the coding process from the content of the interviews. The sub-themes were divided into several categories that became primary themes for this study. Most of the primary themes (Management Support, Self-Efficacy, Perceived Barrier, Trust, Perceived Severity, Perceived Susceptibility and Perceived Benefit) were also shown to be significant factors that influenced the users' compliance behaviour towards HIS security policies.

6.5.1 Management Support

Management support in this qualitative study concerns a wide array of perceptions regarding implementation of the ISPs relating with HIS uses through HIS prototype.

Currently, the hospital ISPs are implemented by the Ministry of Health (MOH) through the Malaysian Administrative Modernization and Management Planning Unit (MAMPU): *"MAMPU is responsible for implementing new policies regarding HIS uses.", said by* participant *(P9)*. Participant *(P9)* also said: "*Currently, I have received ISPs notifications via email. I feel that the implementation of ISPs thru online announcement and notification messages is better."*

Based on the interview content, the current process for delivering the ISPs starts from top management (Hospital Director) and the top management will hand over the responsibility to the Head of Department (HOD). Then, the HOD is responsible for delivering the email to all the staff within their department. Participant *(P11)* said: "*If new policies are implemented, the top management will email the information to our head of department (HOD), and then the HOD will forward the email to us."* Another participant said that the IT administrator is responsible for notifying all staff regarding the new policies relating to HIS uses. Participant *(P14)* said: *"Currently, Information Technology (IT) management will email us of anything related to information security policies or Health Information System uses. So, I will read the email to find out about the current policy and this will help me to be alert about the issues."*

Most of the participants reported that they were satisfied with the proposed system because they can retrieve the information about current security policies faster compared to the current practice (email). One participant *(P13)* said, *"The system is faster than email because we can read it immediately after logging in."*Another participant *(P1)* said, *"I am satisfied with the online announcement system because I can get the information about new policies and information security threats faster."*

Moreover, the ISPs can also be obtained from the hospital e-portal; one participant *(P1)* said, "*I noticed that management has placed the ISPs document on the hospital portal. So, I can retrieve it from there. Just sometimes it depends on whether or not I want to read it."* Apart from that, participants also reported that they are aware of hospital ISPs during the e-patuh test. Participant *(P2)* reported as follows: *"I am aware of the security policies through the e-patuh test. This test is conducted to evaluate our understanding towards ISPs implemented by the MAMPU."*

Most of the participants in this study also agreed that the e-patuh test currently conducted by MAMPU is aimed to evaluate their understanding concerning information security compliance behaviour. This test helps them be aware of the information security compliance issue. Therefore, the proposed system will help them to be alert about when they need to take the test. Participant *(P11)* reported as follows: *"All hospital staff who are also HIS users need to take the e-patuh test. This test is conducted to evaluate our understanding towards the ISPs. If the proposed system is implemented in the hospital, then the process of taking e-patuh test is more convenient."* Similarly, another participant *(P12)* also said: *"Recently, I did the e-patuh test. This test is compulsory for all staff and I feel the proposed system will help me to be alert about the test."*

The participants also expressed their satisfaction with the proposed system, since they did not satisfy with the process of ISPs distribution that currently practiced in the hospital. Participant *(P1)* said: *"We can retrieve the ISPs through the hospital intranet portal. We can also view the ISPs document online. My concern is that the hospital management was not informed about information security incidents or threats formally.*

So, I was not aware about this." Meanwhile, another participant *(P18)* also reported as follows: *"Hospital management should understand the problems of the staff, such as whether the staff understand the policies or not. They always think that staff know about the current policy, but, actually, they do not. So, it is important that the management clarify the importance of the security policies that are implemented in the hospital. I think the proposed system able to reduce this problem."*

Moreover, the participants also stated that the management should take the ISPs implementation issues seriously, as many of the employees in the hospital were not aware about the current policy and they did not receive it formally as they were supposed to. This issue was reported as follows: *"I did not receive any ISPs and the ISPs were not informed formally. I think management should seriously think about the ISPs implementation issue. They should distribute the information about new policies to all staff effectively and I feel that the proposed system might help." (P12)*.

In terms of controlling and monitoring employees' behaviour, the interview content shows that the participants mentioned about the password management that is currently practiced in the hospital, such as HIS users are required to update the password they use for accessing HIS every three months, otherwise the system will automatically reset their password. Participant *(P2)* said: *"Hospital management enforced the password policy. For example, for the internal system, we are required to change the password every three months."* Participant *(P12)* also mentioned the same thing, as follows: *"I will update my password every three months as it was enforced by the management. The system will detect our password expiration date. So it will automatically reset and we need to update it."* All staff will be alerted of the password expiration date, as reported as follows: *"Usually, I just update my password when it expires. IT staff will email me to alert me about the password expiration date."(P12).*

In respect of another policy regarding HIS access, one participant reported that each HIS user has their own level of authority access, which is based on their job position, as not everyone can access the patients' data. One participant *(P11)* said, *"We cannot simply access hospital data. The HIS has the authority to give access based on job position."*

However, one of the participants *(P12)* said that she was dissatisfied with the way the hospital management handled the information security issue: "*As stated in the policies, we need to log off of the PC after we use it. But, some people are still not practicing it because they have forgotten or are not aware about it because of the lack of control by the management. I also noticed that the management are not really monitoring their staff regarding handling health data. There is not enough staff to control and monitor users' behaviour."*

In terms of the behaviour of superiors, the interviewees agreed that their HODs always encourage their staff to practice information security behaviour and inform their staff about ISPs or any news relating to information security issues. This was reported as follows: *"During department meetings, our HOD will always remind us to practice the security behaviour, such as always log off of our computer if we do not use it and frequently change our password." (P8).* Participant *(P13)* said: *"My HOD is responsible for emailing us about anything related to ISPs. If the email is serious, HOD will email it again and remind us many times."* Participant *(P13)* also said: *"My HOD will always remind all staff about protecting our computer and patients' records."* Even though the superior does encourage staff to practice proper information security behaviour, one of the participants *(P3)* reported that most of the staff were not alerted about any information security incidents that existed in their department. *"My superior always reminds me to log out of the computer after work or if I am not around.*

However, I have not been informed about any security incidents that exist in the hospital. So, this sometimes makes me ignore certain rules, such as not logging off the computer because I feel safe."

In addition, one participant reported negatively about the way hospital management handled information security behaviour among HIS users. Participant *(P10)* reported as follows: "*I have not seen the hospital management motivate staff to comply with the policies. I think the leader should always encourage staff to practice information security behaviour."*

In terms of the security training and awareness campaign, most of the participants said that they only attended training that related to HIS use, but that no training related to ISPs was conducted by the hospital management. Participant *(P4)* said: *"I have worked in this hospital for more than four years and as far as I am concerned, I have only attended HIS training."* Meanwhile, participant *(P13)* said: *"I do not think that there is any ISPs training being conducted in this hospital except HIS training.* Participant *(P7)* argued that the ISPs training is important because it helps them to better understand the content of the policies: *"I also noticed that some staff have difficulty in understanding the policies as some parts of the content are hard to understand. This is something that needs to be explained by an expert, so that everyone can understand it better and know how to practice it. So, I really hope that the training conducted by the management includes this matter."*

Moreover, one of the participants reported about ISPs distribution during HIS training as follows*: "The IT staff have distributed the ISPs during HIS training. The training covers how to use HIS, the Internet and also the security part. This is a compulsory three-day training course. Everyone must attend the training."(P5).*Other participants also mentioned about the effectiveness of HIS training. Participant *(P7)* said: "*I believe that the training regarding these policies is necessary to be conducted for all staff in this hospital and it should be more effective.*" This is also supported by another participant *(P12)*, who said: "*All staff need to attend HIS training. I think the current training is effective.*"

The participant also mentioned about the benefit of having a security campaign, in that a security awareness campaign is able to increase users' awareness regarding the importance of complying and practicing information security. However, an information security awareness campaign was not implemented in the hospital, as reported by participant *(P6)*: *"Currently, the hospital does not have any awareness campaign; maybe if the awareness campaign is implemented through an online portal, it might reduce the compliance behaviour issue."*

Thus, it is very important that the hospital management take the security issue seriously. Monitoring is one of the methods to overcome the problem, as reported by the following participant *(P3)*: *"I have no problem reading online messages, it depends on our attitude; as we either want to read it or we do not and just ignore it. Usually, people ignore it if they are busy. But, if management monitor this, we have no choice, we must read."*

6.5.2 Self-Efficacy

This theme focuses on how users feel on their ability towards information security and how the HIS prototype able to improve Self-Efficacy among HIS users.

In terms of the ability to use security tools, the majority of the participants reported that currently, they depend on the IT staff if anything happens to their computer. For example, if the computer is affected by a virus or system error. The participant (P7) expressed this as follows: *"If anything happens to my computer or the system itself, I will refer to the IT staff and ask them to solve the problem. For example, I was careless when keying in patients' data, and wrong data were keyed into the system. As I had difficulty recovering it, I asked the IT staff to retrieve the data and correct it."* Similarly, another participant (P8) reported as follows: *"So far, in this hospital, if we find any system error like a virus, we just call IT staff. Usually, I do not try to fix the computer myself. If I want to update my anti-virus software, I will ask IT staff to do it."*

The participants also stated that the IT staff are always available to assist them with anything related to IT works. Participant (P12) said: *"IT staff are on call (24 hours). If there is any problem with the system, I will call them."* P12 also mentioned: *"I understand a little bit about information security threats, but I have no problem with that since I get help from IT staff because they are helpful. I usually depend on IT staff regarding updating anti-virus or any data error that exists in the system."* Having this issue in mind, the proposed prototype introduced online training that can help HIS users to increase their skills towards information security and most of the participants express their satisfaction with the system because the online training can be attended at anytime and anywhere.

In terms of the ability to obtain and understand ISPs, the majority of the participants reported that they are able to retrieve the ISPs from online system and have no problem reading and understanding the documents via online system. The problem is that of users' attitude. Users are the ones who make a choice whether they want to read it or ignore it. Usually, this is because the users do not have enough time to retrieve the document or even read it. Participant (P18) said: *"I am able to retrieve the ISPs from online announcement system and I am able to read it online. It is just that people will* *take it lightly or they do not bother with it. Perhaps, they have no time to read it like me."* Meanwhile, participant *(P10)* said: *"I have no problem in understanding the ISPs and why we need to comply with them. The ISPs are important and all staff are responsible for reading the ISPs distributed by the management."*

6.5.3 Perceived Barrier

This theme focuses primarily on the barriers to use the HIS prototype among HIS users.

In terms of the communication channel barrier, the participants also argued about the barriers to distributing ISPs via email, inasmuch as some of them were not receiving the email. Participant *(P12)* said: *"Sometimes, staff did not receive the email and they did not get the information properly."* Others reported that even though they received the email containing the ISPs, it was difficult to read the email because the information contained within it was long. *"I do receive the emails, but, usually, I do not read it in detail, just glance through because it is too long. If the email is important and related to my job, then I will read it."(P11)*. Another participant *(P6)* said: *"It is very difficult to read emails that contain long information."*

Therefore, most of the participants reported that they were satisfied with the proposed system because they can retrieve the information about current security policies faster compared to the current practice (email). One participant *(P13)* said, *"The system is faster than email because we can read it immediately after logging in."*Another participant *(P1)* said, *"I am satisfied with the online announcement system because I can get the information about new policies and information security threats faster."*

In terms satisfaction related to easy to access, the participants reported as follows: *"The online announcement system looks easier than email. I am satisfied with the system."(P7)*. Meanwhile, another participant *(P5)* said: *"I am satisfied with it because it contains information related to my work that I should read."*

The participants also reported that the emails are not effective because they usually receive many emails at a time. This was reported as follows: *"This is because, if the information is emailed to us, it takes time for us to read because sometimes we receive a number of emails at the same time."(P7)*. While another reported: *"I seldom check my email, if the emails are too many, it takes time for me to go through one by one. Therefore, I would prefer the proposed system compare to email."(P4)*.

In terms of the quality of the ISPs content, one of the participants *(P9)* reported as follows: *"I am not satisfied with the proposed system because it is not necessary, and is too long-winded."* Meanwhile, in terms of staff position, one of the participants commented that the online message should be updated and that the language used should be conveyed to all staff since they have different positions and levels of education. He said: *"I think the system is good for top level positions but not for lower level staff as mentioned earlier."(P17)*.

Apart from that, the participants also reported that staff, like nurses, need to share a computer, especially if they are working in the hospital wards. This might interrupt getting the online message since many of them share the same computer and use the same password on the same computer. *The participant (P17) reported, as follows: "Online messages are quite difficult because this hospital has a limited number of terminals and a number of employees is large. Usually, nurses who work in the hospital wards will share the computer."*

Moreover, this study also found that a few participants argued about the connectivity of the hospital Internet. They feel that the current Internet system will interrupt the process of getting the online announcement message properly. Participant *(P18)* reported as follows: *"My concern is the Internet System; if the system is slow and not working properly, it should be no problem to have online pop up messages."* Meanwhile, participant *(P6)* said: *"I have no problem with online message, but the problem is that the Internet system at this hospital is quite slow and might interrupt the process."* This is also supported by participant *(P15)*, who said: *"I have no problem with the online announcement system, but my worry is that the Internet system that we have in this hospital is too slow."*

6.5.4 Trust

Trust was another theme raised by the participants, which primarily concerns a wide array of perceptions regarding trust in the organization if the proposed system implemented in the hospital. In terms of trust in people, many participants showed that they trust their colleagues. Therefore, they feel that the security issue is not a big problem, which causes non-compliance security behaviour. Participant *(P14)* said: "*All the staff have their own password, thus I do not see any problem with data missing or other person accessed into HIS using our password without our permission."* Meanwhile, another participant *(P2)* said: "*I believe that the ITD staff will take care of any security threat problem, so I do not bother about the security threats as long as I do my work well."*

In terms of trust in management, most of the participants argued that they should comply with the security policies because it was implemented by MAMPU, and as instructed by MOH. They believe that the implementation of ISPs via online announcement system help increasing their confidence level with the hospital management.

Participant *(P5)* said: *"If this policy was written and implemented by MOH, so then we have no query, we must follow the policies."* Meanwhile, participant *(P1)* said: *"I have no problem complying with the policies because I believe that these policies were implemented by the government and that it is important for us to comply with them."*

Moreover, the participants believed that the government had already done the research about HIS security, thus, they have no reasons not to trust all the policies related to the use of HIS. Participant *(P7)* said: *"I am truly confident in all the policies that are implemented by the ministry as I know that the ministry undertook research before the policies were written. They are also experts regarding this issue."* Similarly, another participant also reported: *"I have no problem complying with the current ISPs because I believe that these policies were written for a certain reason and that the management want to protect hospital data as the data are confidential. Thus, it is essential for us to comply with all the policies for the sake of protecting the data."(P3)*. This is also stated by another participant *(P12)*, who said: *"I do not think the security policies are troublesome, because it was implemented by MAMPU, as government staff, we need to follow it without any doubt."*

Moreover, the interview content also quotes about users trust in the hospital ISPs. If they think that the ISPs are worth following, then the non-compliance issue should not be a problem anymore. The participants mentioned that: *"I trust the policies given by the management because they are logical and I see the objective of having the policies."* *(P13)*, while participant *(P12)* said: *"I must comply with the ISPs because* *these policies were implemented to protect hospital records, and sometimes these records need to deal with the legal process."* Thus, because of this purpose, *"I should comply with the policies and practice them."* Another participant also stated: *"I believe that the ISPs are logical and suitable to be implemented in the hospital since all the works were done through the HIS system. Thus, security is important."(P12)*.

Some of the HIS users trust in the security technology implemented in the hospital, they do not bother with the security issue. Participant *(P4)* said "*I trust in the security system implemented in the hospital, so I do not feel that health records can be hacked easily."* Another participant *(P3)* said: *"I never scan files I download from internal email because I trust in the current internal security."*

6.5.5 Information Security Awareness: Perceived Severity, Perceived Benefit and Perceived Susceptibility

The information security awareness discussed about how the proposed prototype will help to improve awareness of the severity of information security threats (perceived severity), awareness of susceptibility of information security threats (perceived susceptibility) and awareness of benefits of security-countermeasure to prevent information security threats (perceived benefit) among HIS users.

The participants reported that the proposed system helped to increase their information security awareness. The participants believed that if their awareness increases, their skill also increases. This, in turn, will lead to better compliance behaviour among users. Participant *(P6)* said: *"If we can get this information faster, then definitely, our knowledge increases and our understanding towards the objective of practicing information security behaviour improves."* Meanwhile, participant *(P12)* said: *"I feel that I am more aware of any update about ISPs or current issues concerning information security threats through the e-announcement system. If we really understand the message, it will definitely increase our knowledge and skills."*

(a) Perceived Severity

Most of the participants were aware of the seriousness of information security threats that caused them to be more careful when handling health data after using the prototype. One of the participants *(P1)* reported: *"I believe that information security threats are serious, so I ensure that I take care of the data as required in the policies."*

Some of the participants also reported that information security threats are serious because it might harm the hospital's reputation and health records. Participant *(P12)* said: "*If we abuse the hospital data, it involves a legal issue and might harm the reputation of the hospital."* Meanwhile participant *(P6)* said: "*It is important for us to think about the consequences of not complying with the policies as our job is processing patients' data and this data is very confidential. If anything happens to the data, it might harm the patient and records' procedure*."This participant also argued that the information security threat exists because of the careless behaviour of staff: "*I found that data errors are one information security threat and it is still a problem because of the carelessness of staff. Usually, if we face this problem, we need to alter the data, which sometimes complicates our work."*

Moreover, the participants were also aware of the consequences of not complying with ISPs, which will avoid deviant behaviour among HIS users. One participant *(P4)* reported as follows: "*I do not want to face any problem with the management, if I do not comply with the policies and if I am caught it will jeopardise my career."* Similarly, participant *(P8)* reported as follows: "*I do not want to be blamed because of my wrongdoing, so I will make sure that I do my job well.*" This was also argued by another participant *(P18)* who said: "*If I leave my computer on, other people might come and use my computer and possibly access the system and read the confidential data. If anything happens, I will be the one who is responsible, not that person.*"

In terms of password sharing, most of the participants were aware of the severity of sharing the password with other people. Participant *(P14)* argued about data abuse: "*Definitely, I am not going to share my password with other staff because I need to avoid any problem in the future, such as that person might abuse the data in the system*" whileanother participant *(P7)* reported as follows: "*I will not share my password with other colleagues to avoid any future problem.*"

Based on the interview content, the participants also stated about being subject to disciplinary action. Participant *(P13)* said*: "I think it is necessary for us to comply with the policies. Otherwise, if anything bad happens, we may be subject to disciplinary action."* Moreover, the participants agreed that they would be penalised by the management if they were subject to disciplinary action. One of the participants *(P11)* reported as follows: *"I realize that if I do not comply with these policies, I will be penalised by management."* Thus, as they perceive the severity of not complying with the ISPs, they will try to avoid any deviant behaviour. One participant *(P11)* said, *"I will not simply share hospital data with unauthorised users. I believe that patients' data is confidential and should be protected to avoid any serious problems. We might get a serious penalty if the data are lost or harmed."*

(b) Perceived Benefit

In terms of the perceived benefit of security-countermeasures, the research findings addressed two sub-themes under perceived benefits (benefits of ISPs and benefits of system security technology).

Based on the interview content, one of the participants reported about the benefits of ISPs as follows: "*ISPs are important and should be implemented in the hospital because hospital data are confidential. The ISPs provide a guideline to users of how to protect health data."(P15).*

Moreover, most of the participants argued about the benefits of security technology tools. One of the participants *(P9)* said, *"The anti-virus software installed in my computer is good and is able to prevent a virus being spread."* Meanwhile, another participant *(P11)* reported: *"In this hospital, we cannot simply access the patient data, the system* (HIS) *recognises the level of authority before allowing a person access into the system based on the password used. So, I think this can reduce security risk.*"

(c) Perceived Susceptibility

The participants reported the probability of information security threats existing in the hospital. Participant *(P14)* said: *"The probability of information security threats existing is high, especially when all the health data are accessible through the online system; if we are not careful enough, like we do not log out from the system after use, other people will access it and look for information".* Another participant *(P17)* also reported as follows: *"Information security is very important for all hospitals that implement HIS, because this system allows confidential health data to be accessed* *online. Moreover, the possibility of the data being leaked through the online system is high, therefore I feel that it is necessary to have an information security system, and, as a user, we are responsible for practising security behaviour properly."*

Moreover, the participants believed that the threats might exist because of staff having to handle the data of many patients. One participant *(P10)* said, *"Security threats might happen because the data of lots of patients are handled. Sometimes, we cannot check any data error immediately. It is sometimes difficult to trace it, especially during system breakdown."*

This study also found that some of the participants reported that they did not agree that the HIS was vulnerable, which would cause information security threats. Participant *(P4)* said: "*I do not feel that health records are easily hacked. Maybe because I have not experienced it."*Another participant *(P18)* also reported the same thing, as follows: "*I do not think that the current system is vulnerable, the thing is that either you as a user want to follow the rules or not. For example, if you do not keep your password properly, other people might use it and access the system without permission."*

6.6 Discussion of Qualitative Findings

Information security behaviour among users is complicated and difficult to control (Parsons et al., 2014; Liginlal et al., 2012). Therefore, qualitative research was used to elicit an understanding of HIS users' compliance behaviour towards HIS security policies through prototype testing. The prototype was developed based on the significant factors in the HISSPC Model that was found during the quantitative research. The qualitative findings showed that all the significant factors (Management

Support, Perceived Severity, Perceived Benefit, Trust, Self-Efficacy and Perceived Barrier) in the HISSPC Model are contributes to HIS users' compliance behaviour towards HIS security policies. Even though Perceived Susceptibility was not found to be significant during the quantitative research, based on the interview data, users' awareness of the susceptibility of information security threats (Perceived Susceptibility) was found to be an important factor in this study as the participants agreed that if they were aware of the probability of existence of information security threats, they would be more careful in handling health data, especially using the online system. Moreover, employees who perceived the susceptibility of threats are more likely to practice information security behaviour properly (Ng et al., 2009). The summary of the qualitative theme findings are shown in Table 6.3.

Table 6.3: Summary of qualitative themes

Participant Code	Quotation	Sub-Theme	Theme
P9	"*Currently, I have received ISPs notifications via email. I feel that the implementation of ISPs thru online announcement and notification messages is better.*"	ISPs implementation	Management Support
P11	"*If new policies are implemented, the top management will email the information to our head of department (HOD), and then the HOD will forward the email to us.*"	Leadership behaviour	Management Support
P1	*"We can retrieve the ISPs through the hospital intranet portal. We can also view the ISPs document online. My concern is that the hospital management was not informed about information security incidents or threats formally. So, I was not aware about this."*	ISPs implementation	Management Support
P18	*"Hospital management should understand the problems of the staff, such as whether the staff understand the policies or not. They always think that staff know about the current policy, but, actually, they do not. So, it is important that the management clarify the importance of the security policies that are implemented in the hospital. I think the proposed system able to reduce this problem."*	Leadership behaviour	Management Support

Participant Code	Quotation	Sub-Theme	Theme
P12	*I did not receive any ISPs and the ISPs were not informed formally. I think management should seriously think about the ISPs implementation issue. They should distribute the information about new policies to all staff effectively and I feel that the proposed system might help."*	ISPs implementation	Management Support
P2	*"Hospital management enforced the password policy. For example, for the internal system, we are required to change the password every three months."*	Leadership behaviour	Management Support
P7	*"If anything happens to my computer or the system itself, I will refer to the IT staff and ask them to solve the problem. For example, I was careless when keying in patients' data, and wrong data were keyed into the system. As I had difficulty recovering it, I asked the IT staff to retrieve the data and correct it."*	Skill	Self-Efficacy
P8	*"So far, in this hospital, if we find any system error like a virus, we just call IT staff. Usually, I do not try to fix the computer myself. If I want to update my anti-virus software, I will ask IT staff to do it."*	Skill	Self-Efficacy
P12	*"I understand a little bit about information security threats, but I have no problem with that since I get help from IT staff because they are helpful. I usually depend on IT staff regarding updating anti-virus or any data error that exists in the system."*	Lack of knowledge	Self-Efficacy
P18	*"I am able to retrieve the ISPs from online announcement system and I am able to read it online. It is just that people will take it lightly or they do not bother with it. Perhaps, they have no time to read it like me."*	Skill	Self-Efficacy
P10	*"I have no problem in understanding the ISPs and why we need to comply with them. The ISPs are important and all staff are responsible for reading the ISPs distributed by the management."*	Skill	Self-Efficacy
P11	*"I do receive the emails, but, usually, I do not read it in detail, just glance through because it is too long. If the email is important and related to my job, then I will read it."*	Difficulty of retrieving the email	Perceived barrier
P6	*"It is very difficult to read emails that contain long information."*	Difficulty to read the email	Perceived barrier

Participant Code	Quotation	Sub-Theme	Theme
P2	*"I believe that the ITD staff will take care of any security threat problem, so I do not bother about the security threats as long as I do my work well."*	Trust with IT staff	Trust
P5	*"If this policy was written and implemented by MOH, so then we have no query, we must follow the policies."*	Trust with the management	Trust
P1	*"I have no problem complying with the policies because I believe that these policies were implemented by the government and that it is important for us to comply with them."*	Confidence with the ISPs	Trust
P7	*"I am truly confident in all the policies that are implemented by the ministry as I know that the ministry undertook research before the policies was written. They are also experts regarding this issue."*	Trust with the management	Trust
P3	*"I have no problem complying with the current ISPs because I believe that these policies were written for a certain reason and that the management want to protect hospital data as the data are confidential. Thus, it is essential for us to comply with all the policies for the sake of protecting the data."*	Trust with the management	Trust
P12	*"I do not think the security policies are troublesome, because it was implemented by MAMPU, as government staff, we need to follow it without any doubt."*	Confidence with the ISPs	Trust
P1	*"I believe that information security threats are serious, so I ensure that I take care of the data as required in the policies."*	Seriousness of security threat	Perceived severity
P12	"*If we abuse the hospital data, it involves a legal issue and might harm the reputation of the hospital."*	Harm the reputation	Perceived severity
P6	"*It is important for us to think about the consequences of not complying with the policies as our job is processing patients' data and this data is very confidential. If anything happens to the data, it might harm the patient and records' procedure*."	Harm the reputation	Perceived severity
P8	"*I do not want to be blamed because of my wrongdoing, so I will make sure that I do my job well."*	Blamed	Perceived severity
P18	"*If I leave my computer on, other people might come and use my computer and possibly access the system and read the confidential data. If anything happens, I will be the one who is responsible, not that person."*	Serious problem	Perceived severity

Participant Code	Quotation	Sub-Theme	Theme
P11	*"I will not simply share hospital data with unauthorised users. I believe that patients' data is confidential and should be protected to avoid any serious problems. We might get a serious penalty if the data are lost or harmed."*	Serious problem	Perceived severity
P15	"*ISPs are important and should be implemented in the hospital because hospital data are confidential. The ISPs provide a guideline to users of how to protect health data."*	ISPs benefit	Perceived benefit
P9	*"The anti-virus software installed in my computer is good and is able to prevent a virus being spread."*	Anti-virus benefit	Perceived benefit
P11	*"In this hospital, we cannot simply access the patient data, the system* (HIS) *recognises the level of authority before allowing a person access into the system based on the password used. So, I think this can reduce security risk.*"	Security tool benefit	Perceived benefit
P14	*"The probability of information security threats existing is high, especially when all the health data are accessible through the online system; if we are not careful enough, like we do not log out from the system after use, other people will access it and look for information".*	Probability of existing	Perceived susceptibility
P17	*"Information security is very important for all hospitals that implement HIS, because this system allows confidential health data to be accessed online. Moreover, the possibility of the data being leaked through the online system is high, therefore I feel that it is necessary to have an information security system, and, as a user, we are responsible for practising security behaviour properly."*	Possibility of data leaking	Perceived susceptibility

Based on the qualitative findings as shown in Table 6.3, the hospital management plays their role in distributing the HIS security policies document implemented by MOH. The security policies are distributed via email and uploaded to the hospital server, whereby HIS users can download the security policies document from the hospital e-portal. However, a number of participants reported that they are concerned about how HIS security policies are conveyed to all employees in the hospital. The participants argued that the security policies were not formally distributed to all HIS users effectively, in that there are a number of HIS users who still do not know of the existence of HIS security policies, and, even though they themselves have received the security policies from the management, there are no clear instructions provided from the IT department.

Additionally, the participants also argued that even though they have received the ISPs from their HOD, the content of the ISPs document was too long and difficult to read, which makes them unmotivated to read the policies. If employees are not motivated to read the policies and do not understand the policies very well, it might lead to ignorant behaviour and protection of the information security might fail (Ifinedo, 2014; Knapp et al., 2009).

Besides motivating employees to read the ISPs distributed to them, hospital management should enforce the HIS security policies to ensure that the process of protecting health data is effective. The public hospitals in Malaysia currently practice the e-patuh test, which is conducted by MOH, with the aim of evaluating the users' understanding of the rules and regulations they should comply with when handling health data using HIS. However, based on the qualitative data, the e-patuh test is not effective since users only read the security policies for the sake of passing the e-patuh test, and do not understand the whole content of the security policies, and, ultimately, they forget what they have read. This is supported by the qualitative findings, which indicated that some participants still do not practice information security behaviour. For example, some of the participants still share their password with other colleagues and do not take logging out the computer after use. Thus, we suggest that hospital management should review how the implementation of HIS security policies or ISPs is being managed. It is important to ensure that all the employees receive the ISPs and their understanding towards the ISPs content is as expected. Otherwise, the same problem will happen in the future.

In addition, the HODs are the leaders of every department in the hospital; thus, they should practice positive security behaviour and always remind all their staff in the department about practicing good security behaviour during meetings. Moreover, every HOD must ensure that all the policies and procedures related to HIS use are put into practice by all employees under their department as this can maintain the effectiveness of ISPs (Johnston & Warkentin, 2008). According to Boss et al. (2009), employees need to perceive that ISPs compliance is important to management. In doing this, hospital management should monitor and control employees' security behaviour and needs to indicate that the management view compliance with the policy as mandatory. In addition, the communication between leaders and their followers must also be effective. Therefore, IT management in public hospitals must provide different channels of communication for increasing the effectiveness of HIS security policies implementation, and, hence, increase HIS security protection.

The proposed prototype is one method to improve the communication between the leaders and all the employees in the hospital. Through the prototype, IT administrators are able to manage and monitor the process of distributing information security announcements to all employees in the hospital who have HIS access. Additionally, based on the prototype testing analysis, the participants were satisfied with the proposed system, whereby they are able to receive the message faster and able to read it easily, as long as the messages are not too long or complicated. Otherwise, if the messages contain too many words and are too long, HIS users might leave the message windows without reading.

HIS training was shown to be an effective method to distribute the security message. Moreover, the training can help users to develop an understanding about ISPs (Waly et al., 2012). Therefore, hospital management should not just conduct training about how to use HIS implemented in the hospital but also conduct training about ISPs related to HIS. The training should also be considered to be conducted through online system because most of the participants were satisfied with online training. This will help to increase users' understanding concerning the contents of ISPs.

HIS users have different levels of education and knowledge, thus, the hospital management are responsible for training users accordingly. Additionally, the ongoing training can also help to increase users' knowledge and awareness, thus improving security behaviour among employees. Moreover, this study also found that the security awareness campaign influences users' compliance behaviour towards HIS security policies. Thus, hospital management should consider implementing security awareness campaigns in the hospital, as, currently, no such campaigns are implemented in Malaysian public hospitals. Previous studies have shown that security campaigns are one of the methods that increase users' security awareness (Albrechtsen & Hovden, 2010; Eminağaoğlu et al., 2009; Rezgui & Marks, 2008).

Moreover, information security awareness (ISA) is able to educate IS users and make them aware of any information security threats and issues, which, sometimes, can have an impact on the users' awareness level (Hovav & D'Arcy, 2012; Kruger et al., 2011) and hospital security culture. Previous studies have explored the significance of ISA among information system (IS) users (Huang et al., 2011; Bulgurcu et al., 2010a). However, contrary to previous studies, the current study has explored the context of ISA in more detail by focusing on several factors based on the Health Belief Model (HBM). The qualitative findings of the current study indicated that users' awareness of the severity of information security threats (Perceived Severity) plays an important role in users' compliance with ISPs. The participants argued that the reason that they comply with hospital ISPs is to avoid any disciplinary action that may affect their career. Moreover, users' awareness about the susceptibility of information security threats (Perceived Susceptibility) also helps them to be more careful when handling health data when using HIS.

The findings indicate that the participants who are not experienced with information security threats, do not consider that the likelihood of the occurrence of information security is high, which causes ignorant behaviour. Having this issue in mind, it shows that the Perceived Severity and Perceived Susceptibility in the context of information security awareness were confirmed as being important factors in influencing users' compliance behaviour towards HIS security policies. If users have good knowledge concerning information security, then they can practice information security behaviour properly and will be more careful when handling health data; hence, security incidents can be decreased. Thus, hospital management should take this issue seriously and implement effective security awareness programmes.

Moreover, this study also found that HIS users are aware of the benefit of security-countermeasures. They realise the importance of updating user passwords and scanning any portable device before connecting it to the computer. The current practice in the Malaysian public hospitals is that the IT administrator sets in place the HIS system, in which, every three months, users are forced to update their current password, otherwise the system will not allow the user to log in to the system using the old password. The password management implemented in the public hospitals is shown to be effective. However, some of the employees still think that this procedure is troublesome. This indicated that some of the employees are not aware of the importance of changing the password regularly. Moreover, lack of understanding towards the security policies cause non-compliance behaviour among employees (Netschert, 2008). Therefore, it is very important to educate employees about the importance of practicing information security behaviour and follow all the rules and regulations related to HIS security adequately.

Based on the prototype testing results, most of the participants were satisfied with the proposed prototype; they believe that the proposed prototype helps to improve their awareness towards information security. This is because every user will receive the HIS security message faster compared to using email, such as information about the latest security policies and information about the latest issues concerning security threats that are distributed by the IT Administrator. Thus, we believe that the proposed prototype is able to overcome the issue discussed above.

Previous studies suggested that Self-Efficacy is an important factor in improving the users' interaction with the computer system, especially using security tools (Rhee et al., 2009; Torkzadeh & Van Dyke, 2002), such as updating anti-virus and encrypted data. Base on the qualitative findings, most of the HIS users depend on the IT staff concerning updating the anti-virus software, system error, etc. Some of the HIS users did not know how to use the current technology, especially users over the age of 40. They also did not know how to resolve the system error or anything related to IT. Health professionals, such as doctors, are busy, thus, they prefer that the IT staff, who can be contacted at any time, handle all the issues related to IT. Moreover, most of the health professionals assume that security is not their responsibility and that it is supposed to be the responsibility of the IT staff. However, the hospital has a lack of IT staff, which has become an issue, in that not all problems can be resolved by them immediately. Therefore, the hospital management should hire more IT staff who can work in shifts to ensure 24-hour coverage since the hospitals are working 24 hours a day. Moreover, it is very important to train HIS users regularly. The training should not just involve how to use HIS but should, among others, also include the training concerning how to resolve system error, how to update anti-virus, and how to recognise security threats. In this study, we suggest that the hospital conducts online training through the proposed prototype. The online training is believed to motivate HIS users to attend the training as they can attend the training anywhere and anytime.

Based on the interview data, Perceived Barrier also play a role in users' compliance behaviour towards ISPs related with HIS uses. HIS users have stated several barriers that make them ignore certain policies if implemented through online, such as the ISPs document containing longwinded information. Their job conditions make them busy most of the time, for example doctors, and, because of time limitations, many health professionals ignore reading the ISPs that they receive either by email or online system, especially if the documents contain longwinded information. Moreover, some ISPs documents are difficult to read for certain users. Therefore, MAMPU and the hospital management must consider improving the ISPs that are currently used. In addition, we suggest that the ISPs be distributed during HIS training and that someone who is an expert should take this responsibility to explain the contents to all HIS users. The policies should be understandable by all level of employees to ensure its effectiveness (Metalidou et al., 2014). Moreover, the contents of ISPs should clearly stated the employee's exact role and responsibilities towards information security.

The IT management enforces all HIS users to update their passwords every three months by sending a password expired notification. However, most of the HIS users face difficulty in memorizing the password, which makes them use the same password every time they are forced to update. With the password management that is currently practiced, it is good to remind HIS users to update the password they use to access HIS. However, HIS users need to be educated about the importance of updating the password, otherwise their security behaviour will remain as it is.

Moreover, HIS users like nurses who work in the ward have to share a computer. In this case, some users might use the same password as the person might forget to log off the current computer. In the current culture in the hospital, most HIS users do not feel that sharing a password violates the security rules, as, sometimes, their work environment is complicated, and, sometimes, breaking some rules is needed. Therefore, it is very important to inform the HIS users that sharing passwords is one of the security violation behaviours that users need to avoid. Thus, again, we suggest that a security awareness campaign should be implemented in the hospital and security education should be conducted regularly and effectively. According to Noor Hafizah Hassan and Zuraini Ismail (2012), "*security cannot be treated as* an *add-on component; security must be given adequate priority*.*"* p. 1009. Thus, all the hospital stakeholders, such as MOH and the hospital board of directors should take this issue seriously.

The computer sharing issue among HIS users, such as nurses, also becomes a barrier to the proposed prototype. The proposed prototype allows the IT administrator to send the information security message to all HIS users; however, HIS users need to log into the system before they are able to receive the message. Then, after the system verifies a user's authentication and status, the online announcement or notification pop-up window interface will appear. The user can view and read the content of the announcements or notifications online before accessing the HIS sub-system. If the HIS users do not log into the system, they will never receive the message. Therefore, the proposed SMS system in this study will help to notify users about the online message.

HIS users should take responsibility for reading the message and hospital management should remind them about this issue.

The qualitative analyses of this study found several sub-themes under Trust that contribute to users' compliance behaviour towards HIS security policies. In terms of trust in technology, HIS users believe that the current technology that hospitals implemented is able to detect any error or prevent any security threat. Therefore, some HIS users always ignore scanning any file downloading from the email or other sources. Moreover, trust in co-workers also allows HIS users to break some rules, such as not logging off the computer if they are not around and sharing their password with other colleagues to ease their jobs. This sometimes happens because HIS users do not experience any information concerning security threats, or they lack security awareness and always feel that their work environment is safe. Even though the hospital has implemented good security technology, the technology can be misused by people; no matter how strong the security system and policies are, there will be a threat to information security should the user fail to adhere to the policy and system (Waly et al., 2012). Thus, it is very important to motivate HIS users to follow the rules and procedures that have been stated in the HIS security policies, otherwise security fails.

On the other hand, trust in management and its policies influence HIS users to follow any rule and regulation that is implemented in the hospital because they believed that it is important for them to adhere to the security policies that are implemented by the government. Some of the employees were not aware of the HIS security policies, and, as no clear instructions had been given to them, they ignore certain policies. Therefore, it is very important that the hospital management are aware of the implementation of ISPs in the hospital. The ISPs should be effectively documented and distributed to all employees in the hospitals. Additionally, in order for employees to feel confident in the security guidelines, so that they are able to practice it as recommended by the MOH, the ISP documents must be easy to understand and presented in simple language either distributed via email or through the online announcement messages developed in the prototype. This is supported by Hone and Eloff (2002), who stated that effective ISPs is an understandable, meaningful and able to convince an employee about the important of handling health information securely.

Additionally, most of the respondents believed that the proposed prototype would increase their level of trust in a positive way. Therefore, the HIS prototype can be a platform to distribute ISPs document or anything related with HIS security. However, the most concern is the writing style of the ISPs document, whereby it should be more attractive, if distributed thru HIS. This study suggested that the content style of ISPs should be further investigated in future study.

CHAPTER 7: IMPLICATIONS, LIMITATIONS AND CONCLUSION

7.1 Introduction

In this chapter, theoretical contributions and practical implications as well as limitations are discussed. Suggestions for future research and development are also considered. Finally, a research conclusion is given.

7.2 Theoretical Contributions

This study makes several theoretical contributions. *Firstly*, this study utilize the approach of human-technical interactions via multidisciplinary theories (Health Belief Model, Theory of Planned Behaviour and Trust) to evaluate the relationship between the integrated social-technical values and actions of compliance towards Health Information System (HIS) security policies among selected Malaysian health professionals. This study introduced a new human behaviour model, namely, Health Information System Security Policies Compliance (HISSPC) model by positing the mediation effect of factors in Health Belief Model (Perceived Severity, Perceived Susceptibility And Perceived Benefit) and Self-Efficacy, while the HIS experience as a moderating variable in the context of security management, which is largely unknown among scholars to investigate HIS security policies compliance behaviour among Malaysian health professionals.

This study also fills the research gap between different constructs of Management Support and compliance behaviour. Although the role of management has been used extensively to evaluate the links between employees’ behaviour and technological effectiveness in the Malaysian culture, none of them has connected managerial support with HIS security effectiveness through compliance behaviour. This study has emphasized the consideration on dual aspects of managerial support (leadership behaviour, cues-to-action and information system security training) in evaluating the patterns of compliance behaviour among health professionals with different durations of HIS usage.

The quantitative analysis revealed that Management Support has a significant impact on health professionals' Self-Efficacy and the Management Support also found to be a primary theme in qualitative analysis. This indicates that the management in Malaysian hospitals plays a role to improve security skills of their employees that is in line with previous studies (Siponen et al., 2014; Madhavan & Phillips, 2010). Moreover, Management Support also influences health professionals' information security awareness in terms of the seriousness of consequences in not complying with HIS security policies (Perceived Severity), risk of information security threats (Perceived Susceptibility) and benefits of security-countermeasure in preventing information security threats (Perceived Benefit).

HIS users agreed that information security training and awareness programme are important. Moreover, if hospital management can provide good training and effective security awareness programme, users' behaviour toward information security can be improved, as well as their skill in using information security tools. Thus, Malaysian public hospital management personnel such as hospital directors and hospital IT managers play an important role in sorting out problems of human errors before developing any policies related with information security. Health sector should invest and spent more in information security training and education to maintain information security awareness in hospitals.

Furthermore, the intervening variables (Perceived Severity, Perceived Benefit and Self-Efficacy) that were highlighted in the current study did mediate the effect in the relationship between the Management Support and user's compliance behaviour towards HIS security policies, while Perceived Susceptibility was shown as insignificant. The mediation effect of HBM predictors (Perceived Severity, Perceived Benefit And Perceived Susceptibility) are might not covered in previous studies related to compliance behaviour towards HIS security policies, as well as Self-Efficacy in the relationship of the Management Support and HIS security policies compliance behaviour.

According to Ng et al. (2009), the motivation for security is to mitigate risks and reduce threat likelihood. Thus, if users perceive security threats is severe and perceive the benefit of using security tools, their motivation to adopt information security behavior is high. Moreover, Herath and Rao (2009a) suggested that if employees perceive higher levels of penalties for non-compliance with ISPs, such as loss of job or heavy fines, their non-compliant behaviour is likely to decrease. It is believed that if health professionals are aware of severity of a threat, then they can prevent this threat from happening. Other studies suggested that effective information security training can increase users' awareness of the benefit of applying security-countermeasure in preventing information security threats (Renaud, 2012). It is very important for HIS users to understand for HIS users understand the use of security tool and how this tool benefits to them. If user's knowledge towards the benefit of security tools increased, they will able to use it properly; hence, non-compliant issues can be avoided and security incidents can be decreased.

Based on the Partial Least Square-Structural Equation Modeling (PLS-SEM) analysis, Perceived Susceptibility was not significant. However, based on the qualitative analysis, Perceived Susceptibility was shown to be one of the factors that contribute to HIS security policies compliance behaviour among health professionals. Eventhough, some of the Malaysian health professionals had perceptions whereby they did not find health data to be susceptible to security risks. This is such maybe because they did not have experience and were not familiar with security threats or they felt that current security technology are able to protect health data. However, this issue needs to be investigated further as the scope of this study is limited to health professionals working at three Malaysian public hospitals.

Based on the data analysis, some of the health professionals lack skills in information security. Self-Efficacy in this study has shown to be one of the significant factors and in line with previous studies. It also has positive influence on employee's compliance behaviour towards information security (Brady, 2011; Herath & Rao, 2009b). Thus, Malaysian hospital management must seriously consider this issue because the HIS users must have skills to adopt information security tools as this can lead to adequate practice of information security behaviour.

This study has found that Perceived Barrier is a negatively significant predictor when applied to HIS's security policies compliance behaviour and majority of the respondents did not find much barriers of inconvenience in complying with the ISPs related to HIS users. Moreover, based on the interview data analysis, the security barriers were the reason of non-compliance behaviour towards ISPs among health professionals; even though most of them are aware of their responsibility to protect health data. The issue is that either they want to put information security into practice in their daily work or just simply to ignore them.

Secondly, the current study is among the first to examine the moderating effect of the HIS experience of Malaysian health professionals between the factors in HISSPC model and HIS security policies compliance behaviour using multi-group analysis. Previous studies have signified that the role of working experience is related to employees' knowledge (Rodgers, Negash, & Suk, 2005) and employees' competence (McHugh & Lake, 2010), which can increase employees' job performance. However, how the employees' experience of using the technology in the hospital impacts on user's compliance behaviour towards HIS security polices implemented in the hospital is still largely unknown. This study proposed a theoretical model to examine the moderating effect of HIS experience among health professionals on the relationship between Management Support and HIS security policies compliance behaviour, mediated by information security awareness and Self-Efficacy.

Based on PLS-SEM analysis, it was found that superior or leader behaviour from Thoery of Planned Behaviour is valid as part of Management Support besides information security training and implementation of ISPs. The results also showed that Management Support strongly influences users' Self-Efficacy for each group. This indicates that hospital management play a vital role in ensuring that all employees have the necessary skills when handling health data using HIS. Furthermore, Management Support was found to strongly influence information security awareness for low experience users but moderately influence high experience users. In line with previous studies, Management Support was found to be important in promoting information security awareness among IS users (Al-Omari et al., 2012a; Warkentin et al., 2011; Brady, 2010)

Furthermore, both groups have a different perspective on Management Support concerning the compliance behaviour of HIS security policies. The comparison between these groups showed that Management Support is very significant in influencing users with low experience, while this support is not significant among high experience users.

Inexperienced users are considered as new employees who try to focus on building their reputation; hence, they are more careful and try to avoid any problems with the hospital management. Moreover, these users will be sent for security training organised by the health institutions. This will help them to be aware of any new policies related to HIS that have been implemented in the hospital. The findings also reported that the difference in the indirect effect of Management Support on users' compliance behaviour between groups was not significant through the extent of all mediation links.

In terms of perceived susceptibility, the multi-group analysis result found the statistical difference between both groups, whereby the awareness of perceived information security threat susceptibility significantly influenced users' compliance behaviour towards HIS policies in the high experience group and that the path was stronger than for users with low experience. This study concluded that HIS users with high experience of HIS are more aware of the importance of complying with HIS policies compare to HIS users with low experience. Therefore, hospital management should focus on making clear to new employees that unsecured practices can lead to security incidents and that such a situation can have dramatic consequences not only for the hospital, but also for the employees. Moreover, the multigroup-analysis results also showed that there is no statistical difference in the standard path between other factors in the HISSPC in the two groups.

Thirdly, this study contributes to the studies of Trust, in the context of the effectiveness of the security policies related with HIS uses. In this study, the Trust factor was shown to be the most influential factor of HIS security policies compliance behaviour for both groups compared to other factors in the HISSPC model. This indicated that the Trust factor is an important factor to be embedded in Malaysian hospital culture to ensure that all hospital employees comply and practise information security behaviour properly as requested by hospital management, which is in line with previous studies (Noor et al., 2013; Smith, 2010).

Meanwhile, the qualitative data analysis found several Trust elements in the context of HIS security policies compliance behaviour (Trust in people, Trust in technology, Trust in management and ISPs). Trust in people or co-workers, and trust in technology might cause non-compliance behaviour among health professionals, whereby they are willing to break some rules such as sharing password with other people that they trust, and did not scanning file downloaded from the email, as they believe that the security technology will do the scanning tasks automatically. IS users must have knowledge towards practicing information security behaviour (Rocha Flores et al., 2014; Xiao, Hu, Croitoru, Lewis & Dasmahapatra, 2010). Lack of knowledge might lead to ignorance behaviour among IS users. Therefore, the hospital management just not ensuring the security policies are put into practice in health institution, but must also ensuring all employees are clear what their exact role and responsibilities concerning information security.

In contrast, trust in management and ISPs have a positive impact to compliance behaviour among health professionals. Thus, the hospital management should document and distribute the ISPs through online effectively and efficiently, whereby the documents can be easily understood, and easily accessed and applied by all employees in the hospital. Furthermore, employees who trust the organization's rules will most likely enjoy working in the organization, and, hence, increase job commitment (Heavey et al., 2011).

Finally, this study uses the mixed-method research (quantitative research, prototype development and qualitative research) approach to test the HISSPC model with the purpose of increasing the validity and the strength of the study, and decreasing the research bias. In this study, the quantitative method was used to determine the relationship between the factors in the HISSPC model and health professionals' compliance behaviour towards HIS security policies. Meanwhile, the qualitative research was employed to explore the findings from a quantitative research in more depth during prototype testing. The HIS prototype was developed based on the significant factors found during quantitative analysis. According to Hesse-Biber (2010), the combination of several approaches in research helps in expanding the understanding of the research problem. Thus, the HISSPC model will be more useful to determine user's compliance behaviour towards HIS security policies.

7.3 Practical Implications

The statistical test results of the current study revealed several practical implications. *Firstly,* top hospital management, such as hospital directors and hospital IT managers, play an important role in sorting out problems of human errors before developing HIS security policies; thus, they should ensure that all employees, both new and old, are given information security training in view of the fact that people tend to forget what they have learnt. Moreover, the training should be conducted regularly and should be enforced to all employees who uses HIS in their daily tasks. Therefore, the uses of online training might help in the future.

Secondly, systematic documentation on the implementation of security policies and procedures with non-technical terms are very important, especially for new comers and low HIS users. This is seen from moderate responses on the technicality, effectiveness and flexible assessment of security policies. Thus, guidelines and procedures should be written clearly with technical and non-technical terms made easy for all level of employees. With clear instructions, they will be able to understand their roles and responsibilities to reduce the risks of security incidents (Metalidou et al., 2014; Doherty, Anastasakis & Fulford, 2009).

Thirdly, the communication between top management and employees should be improved. Management at different levels should use multiple channels such as emails, alerts of websites, SMS notifications and social networking tools (Skype, Facebook, LinkedIn and so on) to assist their employees through the dissemination of latest updates about security threats and new policies on the security of health data. This would encourage health professionals to attend the available security trainings.

Next, Malaysian hospitals should consider the experience of health professionals in using HIS and try to understand employees' particular motives in complying with HIS policies. Based on the research results, low HIS users have reflected serious disappointments on the incomplete packages of information system security training such as updates on the changes of information security policies, distribution of articles or newsletters on the security and system tools that have expanded lack of acquisitions of skills in protecting the organizational data. This shows that HIS users with high usage of HIS were using alternative means to increase their skills to maintain continuous probability of compliance towards security policies. Therefore, members of hospital management such as board of directors and IT managers should improvise the effectiveness of security training programmes on a regular basis to satisfy the needs of Self-Efficacy among low experienced health professionals.

Finally, information security awareness campaigns should be promoted to ensure that employees do not forget their responsibility to comply with ISPs related with HIS uses and to keep abreast of the latest information security threats. Employees are just normal human beings who tend to forget. Therefore, they need to be alerted and informed many times.

7.4 Limitations and Future Research

Several limitations were found in this study. *First*, the focus of this study has been limited to selected health professionals and Malaysian public hospitals. The procedure to get an approval to conduct a research at Malaysian public hospitals was too rigid and lengthy approval process. Hence, because of time limitation, this study was not able to get many health professionals to participate in the research. Future studies could incorporate larger samples of health institutions and patients for a holistic generalization and systematic presentation of the findings. Malaysian health professionals might have different perceptions towards complying with HIS security policies, thus, it is important for researcher to bring to lightmore issues especially by considering Malaysian culture as influencing factor.

Next, the current study collected data from self-reports that may result in common method variance (CMV). However, this outcome cannot be avoided because of social desirability and the respondent’s consistency motif (Podsakoff & Organ, 1986). The current study has verified that CMV did not influence the data and the data is acceptable. However, future research should enhance the research technique used in this study to obtain more data and explore more factors in studying users’ compliance behaviour towards the HIS security policies.

Moreover, gender was also the limitation in this study; as this study has some difficulties to get more male participants to participate in the survey and prototype testing. This study suggests that future research should gather more male respondent.

Further, this study reflected HIS experience as the only moderating variable in influencing the associations between human-technical interactional factors and compliance behaviour towards HIS security policies. There are other moderating variables such as age, gender, and level of education that could be tested in future studies.

7.5 Conclusion

The integration research model (HISSPC model) by focusing on Management Support and human-technical factors are valid based on PLS-SEM analysis and interview data analysis. The PLS path analysis revealed that majority of the constructs in the HISSPC model affected user's compliance behaviour toward HIS's security policies except for Perceived Susceptibility. In contrast, all the factors in HISSPC model were shown to be significant in qualitative analysis.

Moreoever, through PLS-SEM multi-group analysis, it is inferred that significant differences between low and high HIS users are tied to Management Support and Perceived Susceptibility in influencing their compliant behaviour towards HIS security policies. This shows that high experience users have higher absorptive capacity to deal with innovation catch up towards the latest development of advanced security tools to reduce the expected risks of security incidents compared to low experience users with system catch up.

This study believes that the research findings can contribute to human behaviour in information system studies and are particularly beneficial to policy makers in improving organizations' strategic plans in information security by emphasizing management and human-technical factor issues, especially in healthcare sectors. Most organizations spend time and resources to provide and establish strategic plans of information security; however, if employees are not willing to comply and practice information security behaviour appropriately, then these efforts are in vain. Hence, the adaptation of Theory of Planned Behaviour, Health Belief Model, and other human-technical factors are essential.

Additionally, lack of study in ISPs compliance behaviour focused on Trust factor and it has showed to be the most significant factor that is related with ISPs compliance behaviour. Therefore, the researchers suggest that Trust factor to be further explored in more detail in future study by considering other elements of trust found during qualitative study.

REFERENCES

Aaron, G. A. (2006). Transformational and transactional leadership: Association with attitudes toward evidence-based practice. *Psychiatric Services, 57*(8), 1162-1169.

Abdul Rahman Ahlan, Yusri Arshad, & Muharman Lubis. (2011). *Implication of Human Attitude Factors toward Information Security Awareness in Malaysia Public University*. Paper presented at International Conference on Innovation and Management, Kuala Lumpur, Malaysia, July 12-15, 2011.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

Akhunzada, A., Sookhak, M., Anuar, N. B., Gani, A., Ahmed, E., Shiraz, M., et al. (2015). Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications, 48*(0), 44-57.

Akter, S., D'Ambra, J., & Ray, P. (2011a). Trustworthiness in mHealth information services: an assessment of a hierarchical model with mediating and moderating effects using partial least squares (PLS). Journal of the American Society for Information Science and Technology, 62(1), 100-116.

Akter, S., D'Ambra, J., & Ray, P. (2011b). An evaluation of PLS based complex models: the roles of power analysis, predictive relevance and GoF index. AMCIS 2011 Proceedings-All Submissions.

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013, 7-10 Jan. 2013). *Information Security Policy Compliance: An Empirical Study of Ethical Ideology*. Paper presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012a). *Information security policy compliance: The role of information security awareness, in AMCIS 2012 Proceedings*, http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/16, Seattle, WA.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012b, 4-7 Jan. 2012). *Security Policy Compliance: User Acceptance Perspective*. Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.

Al-Qeisi, K. I. (2009). *Analyzing the Use of UTAUT Model in Explaining an Online Behaviour: Internet Banking Adoption.* Brunel University, Brunel.

Al-Salihy, W., Ann, J., & Sures, R. (2003, 21-24 Sept. 2003). *Effectiveness of information systems security in IT organizations in Malaysia.* Paper presented at the Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432-445.

Alemdar, H., & Ersoy, C. (2010). Wireless sensor networks for healthcare: A survey. *Computer Networks, 54*(15), 2688-2710.

Alhabeeb, M., Almuhaideb, A., Le, P. D., & Srinivasan, B. (2010). *Information Security Threats Classification Pyramid.* Paper presented at the 24th International Conference on Advanced Information Networking and Applications Workshops.

Ali, F. A. B. H., & Aydah, S. M. (2012). Development of Prototype Chat System Using Mobile Platform for Disable People. *Procedia - Social and Behavioral Sciences, 57*(0), 33-39.

Aniza Ismail, Ahmad Taufik Jamil, Ahamd Fareed A. Rahman, Jannatul Madihah Abu Bakar, Natrah Mohd Saad, & Hussain Saadi. (2010). The implementation of hospital information system (HIS) in tertiary hospitals in Malaysia: A qualitative study. *Malaysian Journal of Public Health Medicine, 10*(2), 16-24.

Aurigemma, S., & Panko, R. (2012, 4-7 Jan. 2012). *A Composite Framework for Behavioral Compliance with Information Security Policies.* Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.

Avolio, B. J., & Bass, B. M. (1988). Transformational leadership, charisma, and beyond expectation. *The Free Press*.

Awang, Z. (2012). *A handbook on SEM* (Fourth ed.). Kota Bharu, Kelantan: Centre for Graduate Studies, University Technology MARA Kelantan.

Bahtiyar, Ş., & Ufuk Çağlayan, M. (2012). Extracting trust information from security system of a service. *Journal of Network and Computer Applications, 35*(1), 480-490.

Bahtiyar, Ş., & Çağlayan, M. U. (2013). Trust assessment of security for e-health systems. Electronic Commerce Research and Applications, 13(3), 164-177.

Bandura, A. (1989). *Social Cognitive Theory* (R. Vasta ed.). Greenwich, CT: Jai Press LTD.

Barakat, E. A. M. N. (2002). *Maternal health Information System Petaling District of Selangor State*. University of Malaya, Kuala Lumpur.

Barclay, D., Higgins, C., & Thompson, R. (1995). The Partial Least Squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration. *Technology Studies, 2*(2), 285-354.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*(0).

Basen-Engquist, K., Carmack, C. L., Perkins, H., Hughes, D., Serice, S., Scruggs, S., et al. (2011). Design of the steps to health study of physical activity in survivors of endometrial cancer: Testing a social cognitive theory model. *Psychology of Sport and Exercise, 12*, 27-35.

Bass, B. M. (1985). Leadership and performance beyond expectation. *The Free Press*.

Bates, C. (2006). *Web Programming: Building Internet Applications* (3rd ed.): John Wiley & Sons.

Beas, M. I., & Salanova, M. (2006). Self-efficacy beliefs, computer training and psychological well-being among information and communication technology workers. *Computers in Human Behavior, 22*(6), 1043-1058.

Becker, G. S. (1968). Crime and punishment: an economic approach. *Journal of Political Economy, 2*(76), 169-217.

Benner, P. (1984). *From novice to expert: Excellence and power in clinical nursing practice*. Menlo Park, CA: Addison-Wesley.

Blaze, M. (1993). *A cryptographic file system for UNIX*. Paper presented at the 1st ACM conference on Computer and communications security. ACM

Boije, H. (2010). *Analysis in Qualitative Research*. Thousand Oaks: SAGE Publications.

Bonar, E. E., & Rosenberg, H. (2011). Using the health belief model to predict injecting drug users' intentions to employ harm reduction strategies. *Addictive Behaviors, 36*(11), 1038-1044.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Boujettif, M., & Yongge, W. (2010, 4-6 Nov. 2010). *Constructivist Approach to Information Security Awareness in the Middle East.* Paper presented at the Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on.

Box, D., & Pottas, D. (2013). Improving Information Security Behaviour in the Healthcare Context. *Procedia Technology, 9*(0), 1093-1103.

Brady, J. W. (2010). *An investigation of factors that affect HIPAA security compliance in academic medical centers.* Unpublished 3411810, Nova Southeastern University, United States -- Florida.

Brady, J. W. (2011, 4-7 Jan. 2011). *Securing Health Care: Assessing Factors That Affect HIPAA Security Compliance in Academic Medical Centers.* Paper presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference.

Braun, V., & Victoria, C. (2006). Using thematic analysis in psychology. *Qualitative research in psychology, 3*(2), 77-101.

Brislin, R. W. (1970). Back-Translation for Cross-Cultural Research. *Journal of Cross-Cultural Psychology 1*(3), 185-216.

Brower, H. H., Lester, S. W., Korsgaard, M. A., & Dineen, B. R. (2009). A Closer Look at Trust Between Managers and Subordinates: Understanding the Effects of Both Trusting and Being Trusted on Subordinate Outcomes. *Journal of Management, 35*(2), 327-347.

Brown, W., Ottney, A., & Nguyen, S. (2011). Breaking the barrier: the Health Belief Model and patient perceptions regarding contraception. *Contraception, 83*(5), 453-458.

Buglar, M. E., White, K. M., & Robinson, N. G. (2010). The role of self-efficacy in dental patients’ brushing and flossing: Testing an extended Health Belief Model. *Patient Education and Counseling, 78*(2), 269-272.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009, 29-31 Aug. 2009). *Effects of Individual and Organization Based Beliefs and the Moderating Role of Work Experience on Insiders' Good Security Behaviors.* Paper presented at the Computational Science and Engineering, 2009. CSE '09. International Conference on.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010a). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quaterly, 34*(3), 523-548.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010b, 5-8 Jan. 2010). *Quality and Fairness of an Information Security Policy As Antecedents of Employees' Security Engagement in the Workplace: An Empirical Investigation.* Paper presented at the System Sciences (HICSS), 2010 43rd Hawaii International Conference on.

Burns, J. M. (1978). Leadership. *New York: Harper and Row*.

Bylund, C. L., Galvin, K. M., Dunet, D. O., & Reyes, M. (2011). Using the Extended Health Belief Model to understand siblings’ perceptions of risk for hereditary hemochromatosis. *Patient Education and Counseling, 82*(1), 36-41.

Carmines, E. G., & Zeller, R. A. (1979). Reliability and validity assessment. Available fromhttp://books.google.com.my/books?id=BN_MMD9BHogC&printsec=frontcover#v=onepage&q&f=false

Cavallari, M. (2011). The organizational relationship between compliance and information security. *Academic Business World, 5*(2), 63-76.

Cavalli, E., Mattasoglio, A., Pinciroli, F., & Spaggiori, P. (2004). Information security concepts and practices: The case of a provincial multi-specialty hospital. *International Journal of Medical Informatics*, 297-303.

Celep, C., & Yilmazturk, O. E. (2012). The Relationship among Organizational Trust, Multidimensional Organizational Commitment and Perceived Organizational Support in Educational Organizations. *Procedia - Social and Behavioral Sciences, 46*(0), 5763-5776.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security, 1*(3).

Chang, A. J.-T., Wu, C.-Y., & Liu, H.-W. (2012, 11-13 June 2012). *The effects of job satisfaction and organization commitment on information security policy adoption and compliance.* Paper presented at the Management of Innovation and Technology (ICMIT), 2012 IEEE International Conference on.

Chang, K.-C., Yen, H.-W., Chiang, C.-C., & Parolia, N. (2013). Knowledge contribution in information system development teams: An empirical research from a social cognitive perspective. *International Journal of Project Management, 31*(2), 252-263.

Chang, P. H. (2011, 10-12 Oct. 2011). *Modeling the Management of Electronic Health Records in Healthcare Information Systems.* Paper presented at the Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2011 International Conference on.

Charmaz, K. (2006). *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. Thousand Oaks: SAGE Publications.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39, Part B*(0), 447-459.

Chenoweth, T., Minch, R., & Gattiker, T. (2009). *Application of Protection Motivation Theory to Adoption of Protective Technologies.* Paper presented at the 42nd Hawaii International Conference on system Sciences, Hawaii.

Chin, W. W. (1998). The partial least squares approach to structural equation modelling. In G. A. Marcoulides (Ed.), *Modern methods for business research*. Mahwah NJ: Lawrence Erlbaum.

Chin, W.W., 2014. Frequently asked questions – partial least squares and PLS-graph, 2000. available from: http://disc-nt.cba.uh.edu/chin/plsfaq/plsfaq.htm; accessed Jan 12, 2016.

Chin, W. W., & Dibbern, J. (2010). An introduction to a permutation based precedure for multi-group PLS analysis: results of tests of differencces on simulated data and a cross cultural analysis of the sourcing of information system services between Germany and the USA. In V. E. Vinzi, W. W. Chin, J. Henseler & H. wang (Eds.), *Handbook of Partial Least Squares: concepts, methods and applications*. Berlin: Springer.

Chiu, C.-M., Hsu, M.-H., & Wang, E. T. G. (2006). Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theory. *Decision Support Systems 42*, 1872-1888.

Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security, 16*(5), 484-501.

Christmas, T. H. (2005). *Using partial least squares approach to predict factors that contribute to the impact of E-folios on pre-service teachers' learning.* Unpublished dissertation, Louisiana State University, Louisiana State.

Chung, N., & Kwon, S. J. (2009). Effect of trust level on mobile banking satisfaction: A multi-group analysis of information system success instruments. *Behaviour & Information Technology, 28*(6), 549-562.

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behaviour *Computer Information Systems,* 20-29.

Claar, C. L. (2011). The adoption of computer security: an analysis of home personal computer user behavior using the health belief model (Doctoral dissertation, Utah State University).

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.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly,* 189-211.

Cox, D. N., Koster, A., & Russell, C. G. (2004). Predicting intentions to consume functional foods and supplements to offset memory loss using an adaptation of protection motivation theory. [doi: 10.1016/j.appet.2004.02.003]. *Appetite, 43*(1), 55-64.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior, 28*(5), 1849-1858

Crespo, Á., Salmones Sánchez, M., & Bosque, I. (2013). Influence of Users' Perceived Compatibility and Their Prior Experience on B2C e-Commerce Acceptance. In T. Matsuo & R. Colomo-Palacios (Eds.), *Electronic Business and Marketing* (Vol. 484, pp. 103-123): Springer Berlin Heidelberg.

Creswell, J. W. (2012). *Educational Research Planning, Conducting, and Evaluating Quantitative and Qualitative Research*. Thousand Oaks: SAGE Publications.

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (Third ed.). London: SAGE Publications, Inc.

Crosby, L. A., Evans, K. A., & Cowles, D. (1990). Relationship quality in services selling: An interpersonal influence perspective. *Journal of Marketing Theory and Practice, 54*(68).

Crossler, R. E. (2010). *Protection Motivation Theory: Understanding determinants to backing up personal data.* Paper presented at the 43rd Hawaii International Conference on System Sciences Hawaii.

Corbin, J., & Strauss, A. (2014). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks: SAGE Publications.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasure and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79-98.

D’Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79-98.

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., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. [doi: 10.1016/j.cose.2009.09.002]. *Computers & Security*, *29*(2), 196-207.

Davison, A. C., & Hinkley, D. V. (1997). Bootstrap methods and their application (Vol. 1). Cambridge university press.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior, 26*, 1739-1747.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of Information Technology. *MIS Quaterly, 13*, 319-340.

De Vaus, D. A. (1995). *Surveys in social research* (4th ed.). St. Leonards, NSW: Allen & Unwin

Debi, A. (2008). Information Security management: A human challenge? *Information Security Technical Report, 13*(4), 195-201.

Delgado, A. H., Norby, B., Dean, W. R., McIntosh, W. A., & Scott, H. M. (2012). Utilizing qualitative methods in survey design: Examining Texas cattle producers’ intent to participate in foot-and-mouth disease detection and control. *Preventive Veterinary Medicine, 103*(2–3), 120-135.

Denscombe, M. (2008). Communities of Practice: A Research Paradigm for the Mixed Methods Approach. *Journal of Mixed Methods Research, 2*(3), 270-283.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2008). Information security: The moving target. *Computers & Security, 28*(3-4), 189-198.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*(6), 449-457.

Doherty, N. F., Leonidas, A., & Heather, F. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management, 31*, 201-209.

Dumortier, J., & Vandezande, N. (2012). Trust in the proposed EU regulation on trust services. *Computer Law & Security Review, 28*, 568-576.

Efron, B., & Tibshirani, R. (1986). Bootstrap methods for standard errors, confidence intervals, and other measures of statistical accuracy. Statistical science, 54-75.

Egea, J. M. O., & Gonzalez, M. V. R. (2011). Explaining physicians' acceptance of EHCR systems: an extension of TAM with trust and risk factors. *Computers in Human Behavior, 27*, 319-332.

Ellen, P. S., Bearden, W. O., & Sharma, S. (1991). Resistance to technological innovations: an examination of the role of self-efficacy and performance satisfaction. *Journal of the Academy of Marketing Science, 19*(4), 297-307.

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report, 14*(4), 223-229.

Eric, M., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*, IEEE Computer Society.

Evans, D. M., & Yen, D. C. (2005). Private key infrastructure: balancing computer transmission privacy with changing technology and security demands. *Computer Standards & Interfaces, 27*(4), 423-437.

Fernández-Alemán, J. L., Sánchez-Henarejos, A., Toval, A., Sánchez-García, A. B., Hernández-Hernández, I., & Fernandez-Luque, L. (2015). Analysis of health professional security behaviors in a real clinical setting: An empirical study. International Journal of Medical Informatics, 84(6), 454-467.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*(3), 541-562.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*: Addison-Wesley.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. Journal of marketing research, 382-388.

Frazer, L., & Lawley, M. (2000). *Questionnaire Design and Administration: A Practical Guide*: John Wiley & Sons Ltd.

Fry, M. L., & Dann, S. (2002). *Message processing: Targetting high at-risk group.* Paper presented at the Proceedings of the Australian & New Zealand Marketing Conference, Melbourne.

Gammage, K. L., & Klentrou, P. (2011). Predicting osteoprosis prevention behaviors: Health Belief and Knowledge. *Health Behaviour, 35*(3), 371-382.

Gathan Narayana Samy, Rabiah Ahmad, & Zuraini Ismail. (2009, 18-20 Aug. 2009). *Threats to Health Information Security*. Paper presented at the Information Assurance and Security, 2009. IAS '09. Fifth International Conference on.

Gathan Narayana Samy, Rabiah Ahmad, & Zuraini Ismail. (2010). Security threats categories in healthcare information systems. *Health Information Journal, 16*(3), 201-209.

Gist, M. E., Schwoerer, C., & Rosen, B. (1989). Effects of alternative training methods on self-efficacy and performance in computer software training. *Journal of Applied Psychology, 74*(6), 884.

Goel, S., & Shawky, H. (2009). Estimating the Market Impact of Security Breaches Announcements on Firm Values. *Information & Management, 46*, 404-410.

Götz, O., Liehr-Gobbers, K., & Krafft, M. (2010). Evaluation of structural equation models using the partial least squares (PLS) approach. In V. E. Vinzi, W. W. Chin, J. Henseler & H. wang (Eds.), *Handbook of Partial Least Squares*. Berlin Springer.

Grant, R. (2005). Building a strong security culture. from http://www.citec.com.au/news/

Griffin, M. A., & Hu, X. (2013). How leaders differentially motivate safety compliance and safety participation: The role of monitoring, inspiring, and learning. *Safety Science, 60*(0), 196-202.

Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. [doi: 10.1016/j.cose.2010.12.001]. *Computers & Security, 30*(4), 208-220.

Guo, K. H. (2012). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security* (0).

Gurung, A., Luo, X., & Liao, Q. (2008). Consumer motivations in taking action against spyware: an empirical investigation. *Information Management & Computer Security, 17*(3), 276-289.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), 377-397.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis: A Global Perspective* (7th ed.). Upper Saddle River, New Jersey: Pearson Prentice Hall.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice, 19*(2, Spring 2011), 139-151.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2013). Partial least squares structural equation modeling: rigorous applications, better results and higher acceptance. [Editorial]. *Long Range Planning, 46*, 1-12.

Hair, J. F. J., Babin, B., Money, A. H., & Samouel, P. (2003). *Essential of business research methods*: John Wiley & Sons: United States of America.

Hanson, J. A., & Benedict, J. A. (2002). Use of the Health Belief Model to Examine Older Adults' Food-Handling Behaviors. *Journal of Nutrition Education and Behavior, 34, Supplement 1*(0), S25-S30.

Harvey, M., Reiche, B. S., & Moeller, M. (2011). Developing effective global relationships through staffing with inpatriate managers: The role of interpersonal trust. *Journal of International Management, 17*(2), 150-161.

Hass, S., Wonlgemuth, S., Echizn, I., Somehara, N., & Muller, G. (2010). Aspects of privacy for HER. *International Journal of Medical Informatics, 2*(1), 34-38.

Haux, R. (2006). Health information systems–past, present, future. *International Journal of Medical Informatics, 75*(3), 268-281.

Haux, R. (2010). Medical informatics: past, present, future. *International journal of medical informatics, 79*(9), 599-610.

Hayes, A. F. (2009). Beyond Baron and Kenny: Statistical mediation analysis in the new millennium. Communication Monographs, 76(4), 408-420.

Heavey, C., Halliday, S. V., Gilbert, D., & Murphy, E. (2011). Enhancing performance: Bringing trust, commitment and motivation together in organisations. *Journal of General Management, 36*(3), 1-18.

Herath, T. (2008). *Essays on information security practices in organizations.* Unpublished 3320381, State University of New York at Buffalo, United States -- New York.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hesse-Biber, S. N. (2010). *Mixed Method Research: Merging Theory with Practice*. New York: The Guilford Press.

Hidayah Sulaiman (2011). Healthcare Information Systems Assimilation: The Malaysian Experience. RMIT University

Hogler, R., Henle, C., & Gross, M. (2013). Ethical Behavior and Regional Environments: The Effects of Culture, Values, and Trust. *Employee Responsibilities & Rights Journal, 25*(2), 109-121.

Höne, K., & Eloff, J. H. P. (2002). What Makes an Effective Information Security Policy? *Network Security, 2002*(6), 14-16.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management, 49*(2), 99-110.

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), 615-659.

Huang, D.-L., Rau, P.-L. P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies, 69*, 870-883.

Huang, E., & Chuang, M. H. (2007). Extending the theory of planned behavior as a model to explain post-merger employee behavior of IS use. *Computers in Human Behavior, 23*, 240-257.

Hunton, J. E., & Beeler, J. D. (1997). Effects of user participation in systems development: a longitudinal field experiment. *MIS Quarterly*, 359-388.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Jakobsen, M., & Jensen, R. (2015). Common Method Bias in Public Management Studies. International Public Management Journal, 18(1), 3-30.

Jenkins, J. L., Durcikova, A., & Burns, M. B. (2012, 4-7 Jan. 2012). *Forget the Fluff: Examining How Media Richness Influences the Impact of Information Security Training on Secure Behavior.* Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.

Jiang, L., & Probst, T. M. (2015). Do your employees (collectively) trust you? The importance of trust climate beyond individual trust. *Scandinavian Journal of Management, 31*(4), 526-535

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher, 33*(7), 14-26.

Johnston, A. C., & Warkentin, M. (2008). Information privacy compliance in the healthcare industry. *Information Management & Computer Security, 16*(1), 5-19.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quaterly, 34*(3), 549-566.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems, 43*(2), 618-644.

Jung, B., Han, I., & Lee, S. (2001). Security threats to Internet: a Korean multi-industry investigation. *Information & Management, 38*(8), 487-498.

Kanai-Pak, M., Aiken, L., Sloane, D., & Poghosyan, L. (2008). Poor work environments and nurse inexperience are associated with burnout, job dissatisfaction and quality deficits in Japanese hospitals. *Journal of Clinical Nursing, 17*, 3324–3329.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*, 139-154.

Karjalainen, M. (2011). *Improving employees' information system security behaviours: toward a meta-theory of is security training and a new framework for understanding employees' IS security behaviour. PhD.* Oulu: The University of Oulu.

Kaushal, S. (2011, 23-24 Nov. 2011). *Effect of leadership and organizational culture on information technology effectiveness: A review.* Paper presented at the Research and Innovation in Information Systems (ICRIIS), 2011 International Conference on.

Keers, R. N., Williams, S. D., Cooke, J., & Ashcroft, D. M. (2013). Causes of Medication Administration Errors in Hospitals: a Systematic Review of Quantitative and Qualitative Evidence. *Drug Safety, 36*(11), 1045-1067.

Kim, C., Tao, W., Shin, N., & Kim, K.-S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications, 9*, 84-95.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*, 544-564.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security, 22*(1), 115-126.

Kline, R. B. (2005). *Principles and Practice of Structural Equation Modeling* (2nd ed.): Guilford Press.

Knapp, K. J., Franklin Morris Jr, R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security, 28*(7), 493-508.

Kogler, C., Batrancea, L., Nichita, A., Pantya, J., Belianin, a., & Kirchler, E. (2013). Trust and power as determinants of tax compliance: testing the assumptions of the slippery slope framework in Austria, Hungary, Romania and Russia. *Journal of Economic Psychology, 34*, 169-180.

Koskosas, I., Kakulidis, K., & Siomos, C. (2011). Examining the linkage between information security and end-user trust. *International Journal of Computer Science & Information Security, 9*(2), 21-31.

Kreicberga, L. (2010). *Internal threat to information security - countermeasures and human factor with SME.* Unpublished Master, University of Technology.

Kreicberge, L. (2010). *Internal threat to information security - countermeasures and human factor with SME.* Unpublished Master, University of Technology.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30*, 607-610.

Kruger, H. A., Flowerday, S., L., D., & T. Steyn, T. (2011, August 15-17). *An assessment of the role of cultural factors in information security awareness.* Paper presented at the ISSA 2011, Johannesburg, South Africa.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Kuo, F.-Y., & Hsu, M.-H. (2001). Development and validation of ethical computer self-efficacy measure: The case of softlifting. *Journal of Business Ethics, 32*(4), 299-315.

Kyobe, M. (2010, 2-4 Aug. 2010). *Towards a framework to guide compliance with IS security policies and regulations in a university.* Paper presented at the Information Security for South Africa (ISSA), 2010.

Launders, I., & Polovina, S. (2013). Chapter 13 - A Semantic Approach to Security Policy Reasoning. In B. Akhgar & S. Yates (Eds.), *Strategic Intelligence Management* (pp. 150-166): Butterworth-Heinemann.

Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22*(8), 685-692.

Lechler, T., Wetzel, S., & Jankowski, R. (2011, 4-7 Jan. 2011). *Identifying and Evaluating the Threat of Transitive Information Leakage in Healthcare Systems.* Paper presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference on.

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity.Computers & Security, 59, 60-70.

Lee, H. W., Ramayah, T., & Zakaria, N. (2012). External factors in hospital information system (HIS) adoption model: a case on malaysia. *Journal of Medical Systems, 36*(4), 2129-2140

Lee, K.-I., & Gould, R. (2012). Predicting congregate meal program participation: Applying the extended theory of planned behavior. *International Journal of Hospitality Management, 31*(3), 828-836.

Lee, Y. J., Kauffman, R. J., & Sougstad, R. (2011). Profit-maximizing firm investments in customer information security. *Decision Support Systems, 51*(4), 904-920.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems, 17*(1), 39-71.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly, 33*(1), 71-90.

Liao, C., Chen, J.-L., & Yen, D. C. (2007). Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: An integrated model. *Computers in Human Behavior, 23*(6), 2804-2822.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security, 28*(3–4), 215-228.

Liginlal, D., Sim, I., Khansa, L., & Paul, F. (2012). HIPAA Privacy Rule compliance: An interpretive study using Norman's action theory. *Computers & Security, 31*(2), 206-220.

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of psychology*.

Lin, K.-M. (2011). e-Learning continuance intention: moderating effects of user e-learning experience *Computers & Education, 56*(2), 515-526.

Lippert, S. K., & Davis, M. (2006). A conceptual model integrating trust into planned change activities to enhance technology adoption behavior. *Journal of Information Sciences, 32*(5), 434-448.

Liu, D., Ji, Y., & Mookerjee, V. (2009). Knowledge sharing and investment decisions in information security. *Decision Support Systems* (0).

Lo, M.-C., Ramayah, T., & Run, E. C. d. (2010). Does transformational leadership style foster commitment to change? The case of higher education in Malaysia. *Social and Behavioral Science, 2*, 5384-5388.

Lorence, D. P., & Churchill, R. (2005). Incremental adoption of information security in health-care organizations: implications for document management. *Information Technology in Biomedicine, IEEE Transactions on, 9*(2), 169-173.

Luethi, M., & Knolmayer, G. F. (2009, 5-8 Jan. 2009). Security in Healt*h Information Systems: An Exploratory Comparison of U.S. and Swiss Hospitals.* Paper presented at the System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on.

Lwin, M. O., Li, B., & Ang, R. P. (2011). Stop bugging me: An examination of adolescents' protection behavior against online harassment. *Journal of Adolescence* (0).

Madhavan, P., & Phillips, R. R. (2010). Effects of computer self-efficacy and system reliability on user interaction with decision support systems. *Computers in Human Behavior, 26*(2), 199-204.

Mahmood Hussain Shah, Hamid Reza Peikari, & Norjaya M. Yasin. (2014). The determinants of individuals' perceived e-security: Evidence from Malaysia. *International Journal of Information Management, 34*(1), 48-57.

Maley, J. F., & Moeller, M. (2014). Global performance management systems: The role of trust as perceived by country managers. *Journal of Business Research, 67*(1), 2803-2810.

Martins, A. (2002). *Information security culture.* Johannesburg: Rand Afrikaans University.

Martin, N., & Rice, J. (2001). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security* (0).

Maru, K., Fujii, Y., Sugita, Y., Ohta, N., & Shiraki, S. (2010). Security of communities based on the e-JIKEI Network with IT and altruism. *Procedia-Social & Behavior Sciences, 2*(1), 88-94.

McDermott, A. M., Conway, E., Rousseau, D. M., & Flood, P. C. (2013). Promoting Effective Psychological Contracts Through Leadership: The Missing Link Between HR Strategy and Performance. *Human Resource Management, 52*(2), 289-310.

McHugh, M. D., & Lake, E. T. (2010). Understanding Clinical Expertise: Nurse Education, Experience, and the Hospital Context. *National Institute of Health (NIH) Public Access, 33*(44), 276–287.

Meillier, L. K., Lund, A. B., & Kok, G. (1997). Cues to action in the process of changing lifestyle. *Patient Education and Counseling, 30*, 37-51.

Mejias, R. J. (2012, 4-7 Jan. 2012). *An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk.* Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.

Merriam, S. B. (2009). *Qualitative Research: A Guide to Design and Implementation*. San Francisco: John Wiley & Sons, Inc.

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*(0), 424-428.

Mitra, J. (2000). Kuhn's concept of the Paradigm. *Management and Labour Studies, 25*(1), 37-42.

Moller, S., Ben-Asher, N., Engelbrecht, K.-P., & Englert, R. (2011). Modeling the behavior of users who are confronted with security mechanisms. *Computer & Security, 30*, 242-256.

MySQL. (2014). Top Reasons to Use MySQL. Retrieved 19 January 2014, from https://www.mysql.com/why-mysql/topreasons.html

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18*(2), 126-139.

Nah, F. F.-H., Siau, K., & Sheng, H. (2005). The value of mobile applications: a utility company study. *Communications of the ACM, 48*(2), 85-90.

Netschert, B. M. (2008). *Information security readiness and compliance in the healthcare industry.* Unpublished 3317887, Stevens Institute of Technology, United States -- New Jersey.

Ng, B.-Y., Atreyi, K., & Yunjie, X. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Noor Hafizah Hassan, & Zuraini Ismail. (2012). A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment. *Procedia - Social and Behavioral Sciences, 65*(0), 1007-1012.

Noor, T. H., Quan Z, S., Zeadally, S., & Jian, Y. U. (2013). Trust Management of Services in Cloud Environments: Obstacles and Solutions. *ACM Computing Surveys, 46*(1), 12-12:30.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). New York: McGraw-Hill.

Nurul Izzatty Ismail, & Nor Hazana Abdullah. (2012, 12-13 March). *An overview of Hospital Information System (HIS) implementation in Malaysia.* Paper presented at the 3rd International Conference on Business and Economic Research (3rd ICBER 2012) Proceeding, Bandung, Indonesia.

Nurul Izzatty Ismail, Nor Hazana Abdullah, Alina Shamsudin, & Nik Azliza Nik Ariffin. (2013). Implementation differences of Hospital Information System in Malaysian Public Hospitals. *International Journal of Social Science and Humanity, 3*(2), 115-120.

Nyhan, R. C. (2000). Changing the Paradigm: Trust and its Role in Public Sector Organizations. *The American Review of Public Administration, 30*(1), 87-109.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31*(5), 673-680.

Pallant, J. (2007). *SPSS Survival Manual: A step by step guide to data analysis using SPSS for Windows* (3rd ed.). New York: McGraw-Hill.

Park, S., Ruighaver, A. B., & Ahamad, A. (2010). *Factors influencing the implementation of information systems security strategies in organization*. Paper presented at the International Conference on Information Sciences and Application.

Parker, D. B. (1981). *Computer security management*: Reston Publishing Company.

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 & Security, 42*(0), 165-176.

Partridge, H. (2005). Digital Divide. *Information security and ethics: social and organizational issues,* 23.

Plotnikoff, R. C., Trinh, L., Courneya, K. S., Karunamuni, N., & Sigal, R. J. (2009). Predictors of aerobic physical activity and resistance training among Canadian adults with type 2 diabetes: An application of the Protection Motivation Theory. *Psychology of Sport and Exercise, 10*(3), 320-328.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*, 879-903.

Podsakoff, P. M., & Organ, D. W. (1986). Self-Reports in Organizational Research: Problems and Prospects. *Journal of Management, 12*(4), 531-544.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Information & Management, 51(5), 551-567.

Poulter, D. R., Chapman, P., Bibby, P. A., Clarke, D. D., & Chundall, D. (2008). An application of the theory TPB to truck driving behaviour and compliance with regulations. *Accident Analysis & Prevention, 40*, 2058-2064.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. Behavior Research Methods, 40(3), 879-891.

Preacher, K. J., & Hayes, A. F. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. Behavior Research Methods, Instruments, & Computers, 36(4), 717-731.

Preacher, K. J., & MacCallum, R. C. (2002). Exploratory factor analysis in behavior genetics research: Factor recovery with small sample sizes. Behavior genetics, 32(2), 153-161.

Prentice-Dunn, S., & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. Health education research, 1(3), 153-161.

Puhakainen, P. (2006). A design theory for information security awarenss. Retrieved 6 Jun 2013 from http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly, 34*(4), 757-778

Purpura, P. P. (2013). 7 - Internal Threats and Countermeasures. In P. P. Purpura (Ed.), *Security and Loss Prevention (Sixth Edition)* (pp. 165-216). Amsterdam: Butterworth-Heinemann.

Redspin. (2013). Breach Report 2013: Protected Health Information (PHI). Retrieved 3 December, 2014, from https://www.redspin.com/docs/Redspin-2013-Breach-Report-Protected-Health-Information-PHI.pdf.

Renaud, K. (2012). Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches? *Security & Privacy, IEEE, 10*(3), 57-63.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: an exploratory study. *Computers & Security, 27*, 241-253.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

Rho, H. O., & Ryu, I. (2011, 26-28 July 2011). *The Impact of Information Technology Threat on IT Appropriation and IT Avoidance.* Paper presented at the Computational Intelligence, Communication Systems and Networks (CICSyN), 2011 Third International Conference on.

Rimal, R. M. (2000). Closing the knowledge-behavior gap in health promotion: the mediating role of self-efficacy. *Health Communication, 12*(3), 22-34.

Ringle, C. M., Wende, S., & Will, S. (2005). SmartPLS 2.0 (M3) Beta. *Hamburg 2005*, from http://www.smartpls.de

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*(0), 90-110.

Rodgers, W., Negash, S., & Suk, K. (2005). The moderating effect of on-line experience on the antecedents and consequences of on-line satisfaction *Psychology & Marketing, 22*(4), 313-331.

Ross, T. P., Ross, L. T., Rahman, A., & Cataldo, S. (2010). The bicycle helmet attitudes scale: using the Health Belief Model to predict helmet use among undergraduates. *Journal of Ameican College Health, 59*(1), 29-36.

Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, 15*(3), 112-133.

Saathoff, G. B., Nold, T., & Holstege, C. P. (2013). Chapter 3 - We Have Met the Enemy and They Are Us: Insider Threat and Its Challenge to National Security. In B. Akhgar & S. Yates (Eds.), *Strategic Intelligence Management* (pp. 24-35): Butterworth-Heinemann.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

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 & Security, 53*, 65-78.

Saidon, I. M. (2012). *Moral Disengagement in Manufacturing: A Malaysian Study of Antecedents and Outcomes.* Unpublished Thesis, Curtin University, Curtin.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-66.

Santos, R., Correia, M. E., & Antunes, L. (2008, 13-16 Oct. 2008). *Securing a Health Information System with a government issued digital identification card.* Paper presented at the Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference on.

Sarkar, K. R. (2010). Assessing insiders threats to information security using technical, behavioural and organizational measures. *Information Security Technical Report, 15*, 112-133.

Schneier, B. (2005). Secret & Lies. *Digital security in a network world*. New York: John Willey.

Sekaran, U. (2003). *Research methods for business* (4th ed.). Hoboken, NJ: John Wiley & Sons.

Seppo, P., Mikko, S., & Adam, M. (2007, Jan. 2007). *Employees' Behavior towards IS Security Policy Compliance.* Paper presented at the System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

Sezgin, E., & Yildirim, S. Ö. (2014). A Literature Review on Attitudes of Health Professionals towards Health Information Systems: From e-Health to m-Health. *Procedia Technology, 16*, 1317-1326.

Shahnawaz, M. G., & Goswami, K. (2011). Effect of Psychological Contract Violation on Organizational Commitment, Trust and Turnover Intention in Private and Public Sector Indian Organizations. [Article]. *Vision (09722629), 15*(3), 209-217.

Sharma, S. K., & Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. *Computers &amp; Security, 26*(4), 290-299.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security, 49*, 177-191.

Shaw, J. B., & Erickson, A. (2014). Destructive leader behaviour: A study of Iranian leaders using the Destructive Leadership Questionnaire. *Leadership, 10*(2), 218-239.

Shaw, R. S., Chen, C. C., & Harris, A. C. (2009). The impact of information richness on information security awareness training effectiveness. *Computer & Education, 52,* 92-100.

Shen, A., Cheung, C., Lee, M., & Chen, H. (2011). How social influence affects we-intention to use instant messaging: The moderating effect of usage experience. *Information Systems Frontiers, 13*(2), 157-169.

Shen, D., Laffey, J., Lin, Y., & Huang, X. (2006). Social influences for perceived usefulness and ease-of-use of course delivery system. *Journal of Interactive Online Learning, 5*(3), 270-282.

Şimşekoğlu, Ö., & Lajunen, T. (2008). Social psychology of seat belt use: A comparison of theory of planned behavior and health belief model. [doi: 10.1016/j.trf.2007.10.001]. *Transportation Research Part F: Traffic Psychology and Behaviour, 11*(3), 181-191.

Singh, P., Fook, C. Y., & Sidhu, G. K. (2006). *A comprehensive guide to writing a research proposal*: Venton Publishing.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43*(2), 64-71.

Siwei, D., & Xiaoping, Y. (2009, 26-28 Dec. 2009). *An Improved Motivation Model for People Behaviors Change in Virtual Communities Based on Social Cognitive Theory*. Paper presented at the Information Science and Engineering (ICISE), 2009 1st International Conference on.

Six, F., & Sorge, A. (2008). Creating a High-Trust Organization: An Exploration into Organizational Policies that Stimulate Interpersonal Trust Building. [Article]. *Journal of Management Studies, 45*(5), 857-884.

Smith, M. L. (2010). Building institutional trust through e-government trustworthiness cues. *Information Technology & People, 23*(3), 222-246.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Suhaila Samsuri, Rabiah Ahmad, & Zuraini Ismail. (2011). Towards implementing a privacy policy: an observation on existing practices in hospital information system. *J e-Health Manag, 2011*, 1-9.

Sun, J., Ahluwalia, P., & Koong, K. S. (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems, 111*(4), 570-588.

Sun, X., Guo, Y., Wang, S., & Sun, J. (2006). Predicting iron-fortified soy souce consumption intention: application of the theory of planned behavior and health belief model. *Journal of Nutrition Education and Behavior, 38*(5), 277-285.

Susanne, F. (2012). *Qualitative Data Analysis with ATLAS.ti* (1st ed.). Thousand Oaks: SAGE Publications, Inc.

Symantec. (2013). Internet Security Threat Report 2013 (Vol. 18).

Tamjidyamcholo, A., Bin Baba, M. S., Tamjid, H., & Gholipour, R. (2013). Information security – Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education, 68*(0), 223-232.

Tan, H. H., & Lim, A. K. H. (2009). Trust in Coworkers and Trust in Organizations. [Article]. *Journal of Psychology, 143*(1), 45-66.

Taylor, S., & Todd, P. (1995a). Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions. *International Journal of Research in Marketing, 12*(2), 137-155.

Taylor, S., & Todd, P. (1995b). Assessing it usage: the role of prior experience. *MIS Quarterly, 19*(4), 561-570.

Tesema, T., Medlin, D., & Abraham, A. (2010, 23-25 Aug. 2010). *Patient's perception of health information security: The case of selected public and private hospitals in Addis Ababa.* Paper presented at the Information Assurance and Security (IAS), 2010 Sixth International Conference on.

Tetlock, P. E., Vieider, F. M., Patil, S. V., & Grant, A. M. (2013). Accountability and ideology: When left looks right and right looks left. *Organizational Behavior and Human Decision Processes, 122*(1), 22-35.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472-484.

Thestar. (2009, July 13). Docs violating patient confidentiality, says NUBE. *thestar online*.

Thomson, K.-L., & von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud & Security, 2006*(5), 11-15.

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 2006*(10), 7-11.

Torkzadeh, G., & Van Dyke, T. P. (2002). Effects of training on Internet self-efficacy and computer user attitudes. *Computers in Human Behavior, 18*(5), 479-494.

Tsai, M.-T., & Cheng, N.-C. (2010). Programmer perceptions of knowledge-sharing behavior under social cognitive theory. *Expert Systems with Applications, 37* 8479-8485.

Uffen, J., & Breitner, M. H. (2013, 7-10 Jan. 2013). *Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions.* Paper presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on.

Ugrin, J. C., & Odom, M. D. (2010). Exploring Sarbanes–Oxley's effect on attitudes, perceptions of norms, and intentions to commit financial statement fraud from a general deterrence perspective. *Journal of Accounting and Public Policy, 29*(5), 439-458.

Unisys Malaysia. (2013). Malaysians More Concerned About Computer Security and Online Shopping But Less Concerned About Physical Security Threats Compared to Five Years Ago - Unisys Security Index finds., from http://www.unisys.com/unisys/mobile/countrysite/news/index.jsp?cid=2200002&id=9700046

Utami, A. F., Bangun, Y. R., & Lantu, D. C. (2014). Understanding the Role of Emotional Intelligence and Trust to the Relationship between Organizational Politics and Organizational Commitment. *Procedia - Social and Behavioral Sciences, 115*(0), 378-386.

van Deursen, N., Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within health care. *Computers & Security, 37*(0), 31-45.

van Maele, D., & Van Houtte, M. (2012). The role of teacher and faculty trust in forming teachers' job satisfaction: Do years of experience make a difference? *Teaching and Teacher Education, 28*(6), 879-889.

van Tassel, D. (1972). *Computer Security Management*: Prentice-Hall, Englewood Cliffs, NJ.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3–4), 190-198.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging The Qualitative-Quantitative Divide: Guidelines For Conducting Mixed Methods Research In Information Systems. *MIS Quarterly, 37*(1), 21-54.

Venkatesh, V., & Morris, M. G. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly*, 115-139.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L., Cook, J., & Eugene Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies, 65*(8), 744-757.

Waly, N., Tassabehji, R., & Kamala, M. (2012, 25-27 June 2012). *Improving Organisational Information Security Management: The Impact of Training and Awareness.* Paper presented at the High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on.

Wang, H., Tsui, A. S., & Xin, K. R. (2011). CEO leadership behaviors, organizational performance, and employees' attitudes. *The Leadership Quarterly, 22*(1), 92-105.

Wang, P. A. (2010, 22-24 June 2010). *Information security knowledge and behavior: An adapted model of technology acceptance.* Paper presented at the Education Technology and Computer (ICETC), 2010 2nd International Conference on.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*(3), 267-284.

Watson, B. (2004). Making Sense of Factor Analysis: the use of factory analysis for instrument development in health care research. Nurse Researcher, 11(3), 91-93.

Watson, E. C., Cosio, D., & Lin, E. H. (2014). Mixed-method approach to veteran satisfaction with pain education. *Journal of Rehabilitation Research & Development, 51*(3), 503-514.

Weirich, D., & Sasse, M. A. (2001). *Pretty good persuasion: a first step towards effective password security in the real world.* Paper presented at the Proceedings of the 2001 workshop on New security paradigms.

Wellington, J., & Szczerbinski, M. (2007). *Research Methods for the Social Sciences*. London, GBR: Continuum International Publishing.

Welsh, E. M., Jeffery, R. W., Levy, R. L., langer, S. L., Flood, A. P., Jaeb, M. A., et al. (2011). Measuring perceived barriers to healthful eating in obese, treatment-seeking adults. *Journal of Nutrition Education and Behavior*, 1-6.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management, 24*(1), 43-57.

Whitten, A., & Tygar, J. D. (1999). *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Usenix Security* (Vol. 1999): Wiley Computer Publishing.

Wiant, T. L. (2005). Information security policy's impact on reporting security incidents. *Computers & Security, 24*(6), 448-459.

Williams, P. A. H. (2009). Capturing Culture in Medical Information Security Research. *Methodological Innovations Online, 4*(3), 15-26.

Williams, P. A. H. (2008). In a 'trusting' environment, everyone is responsible for information security. *Information Security Technical Report, 13*(4), 207-215.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication, 800*, 50.

Wood, C. C., & Banks Jr, W. W. (1993). Human error: an overlooked but significant information security problem. *Computers & Security, 12*(1), 51-60.

Woodhouse, S. (2007, 16-19 Oct. 2007). *Information Security: End User Behavior and Corporate Culture.* Paper presented at the Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on.

Woon, I. M. Y., & Kankanhalli, A. (2007). Investigation of IS professionals' intention to practise secure development of applications. *International Journal of Human-Computer Studies, 65*(1), 29-41.

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). *A protection motivation theory approach to home wireless security.* Paper presented at the Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas, NV.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Wu, Y., Stanton, B. F., Li, X., Galbraith, J., & Cole, M. L. (2005). Protection Motivation Theory and Adolescent Drug Trafficking: Relationship Between Health Motivation and Longitudinal Risk Involvement. *Journal of Pediatric Psychology 30*(2), 127-137.

Wylder, J. (2004). Strategic Information Security. *Auerbach/CRC Press LLC*, pp1-16, 139-153.

Xiao, L., Hu, B., Croitoru, M., Lewis, P., & Dasmahapatra, S. (2010). A knowledgeable security model for distributed health information systems. *Computers & Security, 29*(3), 331-349.

Yap, C. S., Soh, C. P. P., & Raman, K. S. (1992). Information system success factors in small business. *Omega 20*(5), 597-609.

Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management, 31*, 360-365.

Yin, R. K. (2009). *Case Study Research Design and Methods*. London: Sage Publications Ltd.

Yong Rhee, K. (2010). Different Effects of Workers' Trust on Work Stress, Perceived Stress, Stress Reaction, and Job Satisfaction between Korean and Japanese Workers. *Safety and Health at Work, 1*(1), 87-97.

Yoshikai, N., Kurino, S., Komatsu, A., Takagi, D., Ueda, M., Inomata, A., et al. (2011, 7-9 Sept. 2011). *Experimental Research on Personal Awareness and Behavior for Information Security Protection.* Paper presented at the Network-Based Information Systems (NBiS), 2011 14th International Conference on.

Younghwa, L. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems, 50*(2), 361-369.

Yukl, G. (2008). How leaders influence organizational effectiveness. *The Leadership Quarterly, 19*(6), 708-722.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330-340.

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. Journal of ConsumerResearch, 37(2), 197-206.

Zhen, S., Yuqiang, F., & Qing, H. (2012, 4-7 Jan. 2012). *How Leadership Styles Impact Enterprise Systems Success throughout the Lifecycle: A Theoretical Exploration.* Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.

LIST OF PUBLICATIONS AND PAPERS PRESENTED

Presentations: Conferences and Symposiums

1. Postgraduate Research Excellence Symposium (PGReS) 2011, 26-27 September 2011.

2. Postgraduate Research Excellence Symposium (PGReS) 2012, 26 September 2012.

3. 2013 2nd International Conference on Emerging Trends in Computer& Information Technology (ICETCIT 2013), January 15-16 2013, Kuala Lumpur, Malaysia.

4. 2014 3rd International Conference on Management and Education Innovation (ICMEI 2014), May 21-22, 2014, in Paris, France.

5. 2014 IEEE Conference on E-Learning, E-Management and E-Services, December 11-12, 2014, Melbourne, Australia.

Conferences Proceedings

1. Norshima Humaidi and Vimala Balakrishnan. 2012. ***The influence of security awareness and security technology on users' behavior towards the implementation of health information system: a conceptual framework.*** *In Proceeding of international conference on management and artificial intelligence, Singapore (Vol. 35, pp. 1-6).*

2. Norshima Humaidi, Vimala balakrishnan and Melissa Shahrom*,* ***Exploring user's compliance behavior towards Health Information System security policies based on extended Health Belief Model,*** *e-Learning, e-Management and e-Services (IC3e), 2014 IEEE Conference on , vol., no., pp.30,35, 10-12 Dec. 2014, doi: 10.1109/IC3e.2014.7081237*

Journal Publications

1. Norshima Humaidi, Noor Azzah Said & Norzaidi Mohd Daud (2011). ***Investigating the relationship of Users' Behaviour and Internal Security Threat towards the Implementation of Total Health Information System (THIS) in Malaysian Medical Institutions.*** *Australian Journal of Basic and Applied Sciences* .Vol 5 (9), pg. 291-297. ISSN: 1991-8178 (ISI)

2. Norshima Humaidi and Vimala Balakrishnan (2012). ***Management Support as a Predictor to Promote Information Security Behavior among Employees.*** International Journal of Information Technology & Computer Science (IJITCS). Vol 7 (2). ISSN No : 2091-1610. (non -ISI)

3. Norshima Humaidi and Vimala Balakrishnan (2013). ***Exploratory factor analysis of user's compliance behaviour towards HIS security.*** Journal of Health & Medical Informatics, Vol 4 (2). ISSN No.: 2157-7420. (non-ISI)

4. Norshima Humaidi & Vimala Balakrishnan, 2015, ***Leadership Styles and Information Security Compliance Behaviour: the Mediator Effect of Information Security Awareness***, *International Journal of Information and Education Technology, Vol. 5 (4), April 2015. (non-ISI)*

5. Norshima Humaidi & Vimala Balakrishnan, 2015, ***The Moderating Effect of Working Experience on Health Information System Security Policies Compliance Behaviour***, Malaysian Journal of Computer Science, Vol. 28 (2), pp 70-92. (ISI-WOS – Teer 4)

6. Vimala Balakrishnan, Norshima Humaidi, Ethel Llyod-Yemoh, 2016, ***Improving document relevancy using integrated language modeling techniques***, Malaysian Journal of Computer Science, Vol 29 (1), pp 45-55. (ISI-WOS – Teer 4)