A DIMENSION-BASED INFORMATION SECURITY CULTURE MODEL FOR INFORMATION SECURITY POLICY COMPLIANCE BEHAVIOR IN MALAYSIAN PUBLIC UNIVERSITIES

AKHYARI BIN NASIR

DOCTOR OF PHILOSOPHY

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : AKHYARI BIN NASIR

Date of Birth : 1 JUN 1977

Title : A DIMENSION-BASED INFORMATION SECURITY CULTURE MODEL FOR INFORMATION SECURITY POLICY COMPLIANCE BEHAVIOR IN MALAYSIAN PUBLIC UNIVERSITIES

Academic Session : SEM 2 2018/2019

I declare that this thesis is classified as:

☐ CONFIDENTIAL	(Contains confidential information under the Official Secret Act 1997)*
☐ RESTRICTED	(Contains restricted information as specified by the organization where research was done)*
☑ OPEN ACCESS	I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

_____	_____
(Student's Signature)	(Supervisor's Signature)
_____	_____
New IC/Passport Number	Name of Supervisor
Date:	Date:

SUPERVISOR'S DECLARATION

We hereby declare that we have checked this thesis and in our opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Doctor of Philosophy.

_____

(Supervisor's Signature)

Full Name : TS. DR. RUZAINI BIN ABDULLAH ARSHAH

Position : ASSOCIATE PROFESSOR

Date :

_____

(Co-supervisor's Signature)

Full Name : DR. MOHD RASHID BIN AB HAMID

Position : ASSOCIATE PROFESSOR

Date :

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

_____

(Student's Signature)

Full Name : AKHYARI BIN NASIR

ID Number : PCC 16001

Date :

A DIMENSION-BASED INFORMATION SECURITY CULTURE MODEL FOR INFORMATION SECURITY POLICY COMPLIANCE BEHAVIOR IN MALAYSIAN PUBLIC UNIVERSITIES

AKHYARI BIN NASIR

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Doctor of Philosophy

Faculty of Computer Systems & Software Engineering

UNIVERSITI MALAYSIA PAHANG

AUGUST 2019

ACKNOWLEDGEMENTS

All praises to the Almighty Allah, the Most Merciful and the Most Benevolent for granting me the ability, strength and courage to persevere throughout this painful, yet wonderful and fulfilling journey. I could never have completed this PhD journey without Him.

I also would like to express my deepest gratitude to Associate Professor Ts. Dr. Ruzaini Abdullah Arshah, my main supervisor who opened the door towards the commencement of this journey; and subsequently guided me throughout the completion of it. Thank you also is not enough to express my sincere gratefulness to my co-supervisor, Associate Professor Dr. Mohd Rashid Ab Hamid who was present with his wisdom and guidance to lead me towards the finishing line of this PhD journey. Hence, I am forever in-debt to both for their involvement and contribution for this achievement.

Additionally, I would like to convey my heartfelt appreciation to colleagues and friends at TATI University College (TATIUC) and Universiti Malaysia Pahang (UMP) who were always available to assist, encourage and pray for me throughout the journey. Without your assistance, encouragement and prayer, the journey might have been more difficult and unbearable.

Most importantly, my lovely wife, thank you for your love and support throughout the hardship and opulence time of our lives together including throughout the period of this journey.

Finally, to the essence of my life, my parents whose prayers and blessings became my lucky charm to complete this thesis.

ABSTRAK

Ekoran daripada peningkatan insiden serangan keselamatan maklumat yang disebabkan oleh tingkah laku pekerja, sarjana dan pakar mencadangkan pewujudan Budaya Keselamatan Maklumat (ISC) yang positif dalam membimbing tingkah laku pekerja untuk mematuhi Dasar Keselamatan Maklumat (ISP) organisasi. Walau bagaimanapun, ianya masih belum jelas tentang apakah aspek atau elemen yang diperlukan untuk satu pembentukan ISC yang positif, khususnya yang berkesan mempengaruhi tingkah laku pematuhan pekerja terhadap ISP. Kajian semasa masih tidak dapat memberikan satu penemuan yang konklusif mengenai pengaruh sebenar ISC terhadap tingkah laku pematuhan ISP dalam mencadangkan satu model ISC yang berkesan boleh mempengaruhi tingkah laku pematuhan ISP. Dimensi dan pendekatan yang tidak konsisten dalam mengonsepkan ISC adalah jurang utama dalam kajian semasa. Kesusasteraan ISC menunjukkan pelbagai set dimensi berbeza digunakan untuk mengonsepkan ISC dari satu kajian ke kajian yang lain. Selain itu, oleh kerana terdapat kajian yang mencadangkan ISC juga bergantung kepada perbezaan budaya dan kebudayaan kebangsaan, penemuan terdahulu juga tidak boleh digeneralisasikan kepada pekerja dan organisasi di Malaysia. Penyelidikan ini menangani isu-isu ini dengan membangunkan satu model ISC berasaskan dimensi untuk tingkah laku pematuhan pekerja terhadap ISP di Universiti Awam Malaysia. Dalam kajian ini, ISC dikonsepkan sebagai satu konsep yang dibentuk oleh tujuh dimensi menyeluruh yang diformulasikan berdasarkan konsep yang diterima secara meluas, iaitu Budaya Organisasi dan ISC. Selain daripada merangkumi semua peringkat dalam dua konsep ini, dimensi yang diformulasikan juga meliputi kebanyakan faktor utama ISC dalam kesusasteraan semasa. Konsep ini disepadukan dengan teori tingkah laku yang paling ketara dalam domain tingkah laku pematuhan ISP, iaitu Teori Tingkahlaku Dirancang (TPB) untuk mengkaji dan mendemonstrasikan keberkesanan konsep ISC baru ini dalam mempengaruhi tingkah laku pekerja terhadap pematuhan ISP. Model ini diuji dan disahkan dalam tetapan Universiti Awam di Malaysia. Satu kajiselidik telah dijalankan menggunakan teknik pensampelan mudah disebabkan homogeniti populasi sasaran. Kajian ini menggunakan Pemodelan Persamaan Struktur (SEM) untuk mengesahkan model penyelidikan. Teknik pemodelan Kuasa Dua Terkecil (PLS) digunakan untuk menganalisis data melalui pakej perisian SmartPLS 3.0. Penemuan menunjukkan bahawa kesemua tujuh dimensi yang diformulasikan adalah relevan dan ketara dalam menyumbang kepada konsep ISC yang digunakan dalam model ini significant (weightage>0.1 and t-values>1.65, p-values<0.001). Konsep ISC yang dibentuk oleh tujuh dimensi ini juga didapati ketara dalam mempengaruhi tingkah laku pematuhan ISP pekerja (R^2=0.449). Penemuan ini mencadangkan bahawa tujuh dimensi boleh digunakan sebagai garis panduan menyeluruh untuk menilai dan mewujudkan ISC yang akan mempengaruhi tingkah laku keselamatan pekerja terutama di universiti awam di Malaysia. Penemuan juga mendedahkan bahawa aspek yang paling ketara dalam menubuhkan ISC yang positif adalah Pengetahuan Keselamatan Maklumat. Selain itu, faktor Sikap, Kepercayaan Normatif dan Kebolehan Kendiri didapati ketara sebagai pengantara dalam hubungan antara ISC dan niat pematuhan ISP pekerja. Penemuan memberikan pengetahuan baru berkenaan isu konsep ISC berasaskan dimensi. Model ini juga boleh digunakan oleh Pengurusan Keselamatan Maklumat (ISM) sebagai garis panduan untuk merancang dan mewujudkan strategi ISC yang berkesan dan meramalkan tingkah laku keselamatan dalam mendapatkan tahap keselamatan maklumat dan sistem yang lebih tinggi dalam organisasi di Malaysia.

ABSTRACT

Due to the increase of information security incidents and attacks caused by employees' behavior, scholars and experts recommended the establishment of a positive Information Security Culture (ISC) to guide employees' behavior towards complying with Information Security Policy (ISP) established in the organization. However, it is still unclear as to what elements or aspects required for a positive ISC formation, which would effectively influences ISP compliance behavior. Current studies still could not provide a conclusive finding on the actual influence of ISC towards ISP compliance behavior for suggesting ISC model that effectively influences ISP compliance behavior. The inconsistency of dimensions and approaches in conceptualizing the ISC are the main gaps in current studies. ISC literature indicates that different sets of dimensions used to conceptualize ISC in various studies. Apart from that, since some studies suggested ISC depends on cultural differences and national culture, previous findings could not be generalized to Malaysian organizations and employees. This research addresses these issues by developing an ISC model based on new formulated dimensions for employee's ISP compliance behavior in Malaysian Public Universities. In this study, ISC was conceptualized as a dimension-based concept formed by seven dimensions formulated based on widely accepted concepts of Organizational Culture and ISC. The formulated dimensions not only covered all levels in these concepts, the dimensions were also covered most of ISC key factors in current literature. This ISC concept then was integrated with the most significant behavioral theory in ISP compliance behavior literature, which is Theory of Planned Behavior to thoroughly examine and demonstrate the effectiveness of new ISC concept in influencing employees' ISP compliance behavior. The model was tested in public university settings in Malaysia, whereby a questionnaire-based survey was conducted to collect data from the employees using convenient sampling technique due to homogeneity of the population. This study employed Structural Equation Modeling (SEM) to validate the research model. Partial Least Squares (PLS) modeling technique was used to analyze the data via SmartPLS 3.0 software package. The findings show that all seven formulated dimensions are relevant and significant (weightage>0.1 and t-values>1.65, p-values<0.001) in contributing towards ISC concept used in the model. The ISC concept based on these seven dimensions was also found to be significant in influencing employees' ISP compliance behavior (R^2=0.449). These findings suggest that seven aspects represented by seven dimensions in the study could be used as guidelines to assess and establish a positive ISC in guiding employees' security behavior in organizations especially in public universities in Malaysia. The findings also reveal that the most important aspect in establishing a positive ISC is Information Security Knowledge. Moreover, behavioral factors of Attitude, Normative Belief and Self-Efficacy were found to be significant in mediating the relationship between ISC and employee's ISP compliance intention. These findings provide new insights and knowledge on standard issues regarding the concept of ISC based on its dimensions. They also provide a clear understanding on ISC influence towards employees' security behavior. The model could also be used by Information Security Management (ISM) as guidelines to plan and establish effective ISC strategies and to predict security behavior in obtaining higher level of information security and its systems in Malaysian organizations.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACT	Actual Compliance
ATT	Attitude
CMB	Common Method Bias
CMV	Common Method Variance
FSKKP	Faculty of Computer Systems & Software Engineering
GDT	General Deterrence Theory
HCM	Hierarchical Component Modeling
HEI	Higher Educational Institution
HOC	Higher-order Construct
ICT	Information and Communication Technology
INT	Intention to Comply
ISA	Information Security Awareness
ISC	Information Security Culture
ISCA	Information Security Culture Assessment
ISK	Information Security Knowledge
ISKS	Information Security Knowledge Sharing
ISM	Information Security Management
ISP	Information Security Policy
IT	Information Technology
LOC	Lower-order Construct
MAMPU	Malaysian Administrative Modernization and Management Planning Unit
MIS	Management Information System
MON	Monitoring
NB	Normative Belief
OB	Organizational Behavior
OC	Organizational Culture
PCM	Procedural Countermeasure
PLS	Partial Least Square
PMT	Protection Motivation Theory
RM	Risk Management

RO	Research Objective
RQ	Research Question
SE	Self-Efficacy
SEM	Structural Equation Modeling
SETA	Security Education, Training and Awareness
TMC	Top Management Commitment
TPB	Theory of Planned Behavior

CHAPTER 1

INTRODUCTION

1.1 Research Background

In today's digital era, information and its systems are critical and they are the most valuable assets to a modern organization in ensuring their survival (Bélanger, Collignon, Enget, & Negangard, 2017; Kolkowska, Karlsson, & Hedström, 2017). These information assets often hold valuable organizational data resources (Cavusoglu, Mishra, & Raghunathan, 2004; Ifinedo, 2009, 2011; Robert, 2011). Every organization has information to be produced, used, stored and managed in accordance to their business nature and operations. Having specific and relevant information can make a massive difference to an organization's efficiency. Therefore, proper and effective management of information security is essential to ensure the organization's survival in conducting their business and activities. Any risk related to information security is a major challenge for the organization since the risks may have direct consequences such as corporate liability, loss of credibility and monetary damage (Alnatheer & Nelson, 2009; Renaud & Goucher, 2014); which can lead to compromisation of the information, its systems and the organizations. Thus, a mechanism of preventive measures onto these information assets called information security is indispensable in ensuring the confidentiality, integrity and availability of the information and its systems.

Normal practice in implementing information security to achieve its objectives is through technology such as installing firewalls, updating anti-virus software, backing up the systems, maintaining and restricting access controls, using encryption keys, using surge protectors, and using comprehensive monitoring systems (Lee & Larsen, 2009; Ryan, 2004; Workman, Bommer, & Straub, 2008). However, these tools and measures only offer technological or technical solution to the problem, and rarely sufficient in

providing total protection of information system organizational resources (Glaspie & Karwowski, 2018; Herath & Rao, 2009b; Masrek, Harun, & Zaini, 2018; Rhodes, 2001; Sasse, Brostoff, & Weirich, 2004; Stanton, Stam, Mastrangelo, & Jolton, 2005).

Focusing on technical aspects of the security, without appropriate consideration of human interaction with the system is evidently inadequate (Alhogail, 2015a; Parsons, Mccormac, Butavicius, & Ferguson, 2010; Tsohou & Holtkamp, 2018) and cannot guarantee a secure environment for the information (Cram, Proudfoot, & Arcy, 2017; Safa, Von Solms, & Furnell, 2016). Most security incidents and abuses were caused by insiders or employees of the organziation (PWC, 2015, 2016). In fact, they are considered as the weakest link in achieving information security and constitutes as internal threat to the organizations (Chen, Ramamurthy, & Wen, 2015; Connolly & Lang, 2013; Mahfuth, Yussof, Baker, & Ali, 2017; Post & Kagan, 2007; Robert, 2011; Stanton et al., 2005; Durbin, 2016; Vroom & Von Solms, 2004; Warkentin & Willison, 2009). Specifically, this is mainly related to their behavior and practice which fail to comply to the organization's information policies and guidelines (Fagade & Tryfonas, 2017; Ifinedo, 2016). Recent Ransomware attacks that were considered as the biggest and the most damaging cyberattack in history (CNN tech, 2017; The Telegraph, 2017) demonstrate behavior is the main factor causing the attack. In this particular case, experts also suggested that employees must always follow all security requirements as documented in Information Security Policy (ISP) to minimize the threats (Cyber Security Malaysia, 2017).

Henceforth, many scholars recommend successful information security depends on effective human behavior in particular the employees' behavior (Kathryn et al., 2017; Siponen, 2005; Stanton, Mastrangelo, Stam, & Jolton, 2004; Stanton et al., 2005; Von Solms & Von Solms, 2004; Vroom & Von Solms, 2004; Workman, 2007). For that purpose, information security scholars suggested for the establishment of a positive Information Security Culture (ISC) to guide and promote security behavior and practices in organization (Alfawaz, Nelson, & Mohannak, 2010; Alhogail, 2015b; Greig, Renaud, & Flowerday, 2015; Lim, Chang, Maynard, & Ahmad, 2009; Mahfuth et al., 2017; Van Niekerk & Von Solms, 2010; Williams, 2009b). Some scholars called this effort as an institutionalization of information security (Dojkovski, Lichtenstein, & Warren, 2007b), and it is originally suggested to address the misuse of information

assets in an organization by the insiders that could lead to various information security threats (Dhillon, 2001; Magklaras & Furnell, 2004). Malaysian government through Ministry of Science, Technology and Innovation (MOSTI) in National Cyber Security Policy (NCSP) also aims to foster national security culture and encourage Malaysian organizations to implement effective Information Security Management (ISM) in improving security behavior and awareness among employees (CyberSecurity Malaysia, 2015). In this case, information security behavior refers to a set of core information security activities that must be adhered to by end-users to maintain information security as defined by ISP (Padayachee, 2012).

Although it is widely accepted that ISC should be implemented to guide employees towards secured behavior and practices as documented in organization's ISP, there are still lack of clear guidelines on how to establish ISC that could effectively influence and improve employees' security behavior. Not many empirical studies and findings are able to provide clear guidelines of a positive ISC establishment. Although few studies on ISC and ISP compliance behavior have provided some significant empirical evidences on the relationship, these studies could not provide a convincing conclusion. This is due to the inconsistency and incomprehensiveness of ISC concept especially in terms of ISC dimensions used in the studies. Since these dimensions actually represent elements and aspects of ISC establishment, therefore ISC concept based on dimension provides more useful findings. Specifically, in the case of examining ISC effects towards ISP compliance behavior, it provides clearer findings on the aspects of a positive ISC.

The main factor of inconsistency in ISC dimensions is due to the way ISC concept is developed and conceptualized. Although most of the time, Organizational Culture by Schein (1992, 1999) is the most used concept to model ISC, the literature indicates other concepts and approaches are also applicable (Pevchikh, 2015). Thus, there is a lack of common understanding of what ISC is (Tolah, Furnell, & Papadaki, 2017) and what are the most appropriate dimensions should be used to represent this concept.

Although some guidelines and standards are available for establishing Information Security Management System (ISMS) such as BS 7799 or ISO/IEC 27001 (International Organization for Standardization, 2017) and OECD (OECD, 2002), they

are not able to provide effective solutions for all organizations. Fagade and Tryfonas (2017) claim that these guidelines are too general to be applied for all types of organizations because of information security requirement differences due to diverse type of organization and culture. Moreover, no evidence is available on its effectiveness to influence employees' security behavior. Therefore, comprehensive guidelines of ISC and its practice for specific type of organization is still remain unclear.

This research addresses the issues of ISC conceptualization and its relationship with ISP compliance behavior in producing a model for academicians' and practitioners' references in understanding, assessing and establishing a positive ISC in organization. An enhanced model of ISC based on new formulated dimensions is developed and validated in order to investigate its relationship with employees' ISP compliance behavior. These dimensions were formulated based on a widely accepted concept of organizational culture by Schein (1992) and ISC framework by Van Niekerk and Von Solms (2006) to cover most ISC key factors in current literature. The model is also integrated with the most significant theoretical behavioral framework in ISP compliance behavior literature which is Theory of Planned Behavior (TPB).

1.2 Problem Statement

Information security scholars and experts believe the establishment of a positive ISC could guide employees' security behavior particularly in adhering to ISP. However, it remains unclear on how to establish this culture because lack of referral model. Some guidelines and standards are available for establishing Information Security Management System (ISMS) such as BS 7799 or ISO/IEC 27001 and OECD. However these guidelines focus on general aspects of information security management and empirical evidences on its effectiveness in influencing employees' security behavior is still lacking. Thus, adopting these guidelines do not guarantee employees' compliance towards ISP established in the organization (Fagade & Tryfonas, 2017).

Several specific problems contributed to the lack of ISC model for ISP compliance behavior are identified in the literature. First problem is the inconsistency in ISC concepts. ISC is discovered to be conceptualized differently according to factors and dimensions in various studies. Hence, this shows lack of agreement on appropriate dimensions that should be used in representing ISC concept (Alnatheer, 2015; Lopes &

Oliveira, 2014; Tolah et al., 2017). Consequently, it leads to lack of ISC model that comprehensively integrates its important key factors (Tolah et al., 2017). Lim et al. (2009); Dhillon, Syed, and Pedron (2016) highlighted various ISC concepts emerged from the numerous theories and models used by ISC researchers. Until now, the issue of ISC conceptualization is still not properly addressed. To a certain extent, too many dimensions involved in representing ISC in various studies and there is no cohesive definition on these dimensions. There is also no agreement on how ISC should be conceptualized and operationalized due to lack of validated approaches in this field (Karlsson, Astrom, & Karlsson, 2015). All these conceptualization issues have caused problems to academicians and practitioners in finding and referring to the right concept in assessing and establishing ISC (Tolah et al., 2017).

Second problem is lack of ISP compliance behavior model that uses ISC as a sole predictor in the model. Most ISP compliance models did not employ ISC as the sole antecedent or determinant by including other constructs in the model. This means that, there are limited findings that clearly show how an employee's ISP compliance behavior could be influenced by ISC. Apart from producing a solid ISC model to predict ISP compliance behavior, these findings are crucial in determining the actual influence of ISC towards ISP compliance behavior. Moreover, ISC conceptualization issue also results in mixed findings for the relationship between ISC and ISP compliance behavior studies. Inconsistent ISC concept and incohesive dimensions to represent ISC concept are common in these studies. Additionally, a number of ISC key factors did not involve in these studies. Therefore, these studies could not provide a conclusive finding pertaining to ISP compliance behavior based on the actual concept of ISC.

Third problem is lack of specific ISC model and framework that directly focuses on human behavior (Mahfuth et al., 2017). Many scholars suggested the goal of ISC is to influence security behavior especially the behavior towards adhering to ISP (Schlienger & Teufel, 2003a; Von Solms & Von Solms, 2004; Vroom & Von Solms, 2004). Therefore, the relationship between these two concepts should be explained from theoretical behavior perspective to obtain clear understanding about the relationship. In other words, previous empirical study is limited in explaining ISC influence towards ISP compliance behavior from behavioral theory perspective. As such, there is a lack of

understanding about the way ISC influences employees' specific behavioral factor, of which eventually influences their ISP compliance behavior.

In ISP compliance behavior literature, several competing theories were employed to explain ISP compliance behavior such as Theory of Planned Behavior (TPB), Protection Motivation Theory (PMT) and General Deterrence Theory (GDT). Compared to others, three main constructs of TPB, which are Attitude, Normative Belief and Self-Efficacy were proven to be the most significant factors in predicting and explaining ISP compliance behavior of employees (Lebek, Uffen, Neumann, Hohler, & Breitner, 2014; Sommestad & Hallberg, 2013; Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). However, it is still unclear how ISC could promote these three desired behavior factors and how important the factors to be promoted in an organization.

In the context of Higher Educational Institution (HEI), there is a lack empirical study that has been done to address the relationship between ISC and ISP compliance behavior, especially in the context of Malaysian public university sector (Hina & Dominic, 2016). There is also lack of ISC model produced specifically for this sector. This sector is still far behind in adopting ISC and has ample amount of information to be put at stake (Hina & Dominic, 2016), According to Privacy Rights Clearinghouse (2011), education industry has the most number of breaches compare to other sectors such as business, government agencies and medical institution. Recent statistics report by Privacy Rights Clearinghouse (2014) still indicated that this sector is among the most impacted by the breaches.

There are many recent reports of attacks that initially caused by the insiders behavior and practices in particular universities (Berita Harian, 2016; Shawn Logan, 2017; The Telegraph, 2017; UCF Data Breach | IdentityForce, 2017). In Malaysia, there are reports of attacks and data breaches happened in public universities (Berita Harian, 2016; Report, 2019; Times, 2019a, 2019b). These attacks have caused various of losses to the students and universities. For example, one of these reports said that a total of 1,164,540 records, belonging to students who enrolled for various courses at that particular universities has been breached and leaked online. These losses would cost the universities in terms of money and reputation. Clearly, this sector needs smarter information security strategies to leverage the business nature of university that

naturally promote teaching and learning. The reason is that this sector operated more towards open culture of "information sharing" (Ayyagari and Tyks, 2012) with all stakeholders and customers compared to other sectors such as banks or government agencies, which is the common practice in business, is to protect trade secrets and intellectual property.

1.3 Research Questions (RQ)

Based on aforementioned issues and problem statements, the following are the research questions needed to be answered in this research:

1. What are the appropriate dimensions should be used to represent ISC based on Organizational Culture concept?
2. What is the model to address the relationship between ISC and ISP compliance behavior?
3. What is the relationship between the formulated dimensions and ISC concept?
    a. Are these dimensions relevant and significant in contributing to the underlying concept of ISC?
    b. Which dimension is the most important in forming ISC concept?
4. What is the relationship between the ISC concept based on formulated dimensions and employees' ISP compliance behavior?
    a. What is the relationship between this ISC concept with employee's Attitude, Normative Belief and Self-Efficacy of ISP compliance behavior?
    b. What is the relationship between these three behavioral factors and ISP compliance intention?
5. What are the roles of Attitude, Normative Belief and Self-Efficacy in mediating the relationship between ISC and ISP compliance intention?

1.4 Research Objectives (RO)

The main objective of this research is to establish Information Security Culture (ISC) model based on new formulated dimensions for employee's ISP compliance behavior. In achieving this ultimate objective, an ISC concept based on a new set of dimensions is formulated to examine its actual influence towards employees' ISP

compliance behavior. Hence, apart from investigating the relationship between ISC and ISP, the dimensions should represent the elements of assessing and establishing a positive ISC that would improve ISP compliance behavior. This research also investigates in detail the relationship between ISC and ISP compliance behavior from the perspective of Theory of Planned Behavior (TPB) to provide deeper understanding about the relationship. The followings are the summary of objectives for this study:

1. To formulate ISC dimensions based on widely accepted concepts of Organizational Culture and Information Security Culture.
2. To develop a model of ISC based on new formulated dimensions for employee's ISP compliance behavior.
3. To validate the formulated dimensions in representing ISC conceptual model.
4. To validate ISC model for employee's ISP compliance behavior in Malaysian public universities.
    a. To examine the relationships between ISC concept with employee's Attitude, Normative Belief, and Self-Efficacy.
    b. To examine the relationships between employee's Attitude, Normative Belief, and Self-Efficacy with ISP compliance intention.
5. To validate the roles of Attitude, Normative Belief and Self-Efficacy in mediating the relationship between ISC and ISP compliance intention.

In summary, the use of term "conceptual model" in Research Objective 3 (RO3) is to represent the ISC concept based on the formulated dimensions in RO1, whereas the term "model" in RO2 and RO4 refers to the whole research model of this research, which is ISC model for ISP compliance behavior. This whole model is the representation of ISC's influence towards ISP compliance behavior.

1.5 Research Scope

This research tests and validates the model in the context of Malaysian public universities based on two main justifications. Firstly, scholars argued that ISC (Connolly & Lang, 2013; Govender, Kritzinger, & Loock, 2016) and ISP compliance

behavior (Hovav & D'Arcy, 2012) depend on national culture. Due to this matter, previous findings on the impacts of ISC towards employees' ISP compliance could not be applied to Malaysian context since those studies were not conducted on Malaysian employees. As such, validation of the model in this research addresses the issue.

Secondly, according to Privacy Rights Clearinghouse (2011, 2014), education industry has the most number of breaches compared to other sectors such as business, government agencies and medical institution. This sector is still far behind in adopting ISC and has ample amount of information at stake (Hina & Dominic, 2016). Considering that ISC also depends on type of organization and there is a lack of ISC model for Malaysian public university, therefore, there is a need to find the best principle of elements or dimensions for ISC establishment in public universities particularly in Malaysia.

1.6 Research Significant

The significant of this research are as the following:

- This research produces a validated ISC concept based on a set of dimensions from the perspective of widely accepted concepts in ISC literature, which are Organizational Culture (OC) and ISC.

- The ISC dimensions formulated consider most ISC key factors identified in the literature. This is important since more researches are required to provide comprehensive view in guiding and integrating important factors impacted ISC (Karlsson & Hedström, 2014; Tolah et al., 2017).

- The dimensions formulated cover all levels in OC and ISC. Therefore, the model produced in this study could be used as a reference model for ISC based on dimensions.

- The study increases content validity of ISC concept by adding new findings on how new formulated dimensions contribute to the concept. It is very crucial to examine this relationship since Ruighaver et al. (2007) argued that security culture is a multidimensional concept that is often investigated in a simplistic manner. It sheds

some light on ISC concept since this area is relatively new and remain largely unexplored and as yet not well understood (Connolly & Lang, 2013).

- This study provides clear-cut empirical findings on how to establish a positive ISC in an organization that would influence employees' security behavior in line with organization's ISP. It provides ISC model for Information Security Management (ISM) especially in Malaysian public universities to cultivate and assess ISC that would significantly influences employees' ISP compliance behavior.

- This study provides more practical solution since ISC was recommended by scholars and experts as an effective organizational effort that considers social factors in promoting information security behavior and practices to manage information security risks (Alhogail, Mirza, & Saad, 2015; Tolah et al., 2017).

- Since this study thoroughly evaluates how the formulated dimensions would influence ISC using Hierarchical Model Assessment technique, it suggests actions to be taken by practitioners to cultivate and assess ISC in influencing employees' security behavior.

- Due to the significance of Theory of Planned Behavior (TPB) and its main constructs of Attitude, Normative Belief and Self-Efficacy in predicting and explaining ISP compliance behavior, this research provides empirical findings on the significance of ISC in promoting these desired behaviors pertaining to ISP compliance.

- The model could also be used as a reference to develop assessment system or audit tools for ISC in the organization, particularly in Malaysian public universities settings. The system could be used to predict and audit employees' compliance behavior based on the current status of ISC as an effort to minimize security breaches in the organization. There is a demanding need for security behavior audit because current audit systems focus more on technical side of information security (Fagade & Tryfonas, 2017).

- As most of the breaches in Educational sectors caused by employees for not complying with ISP, this study is crucial because it develops ISC model for this sector, especially for Malaysian publis universities.

- ISC model in the study could further assist the management in strategizing the best security solution for university digital culture environment in moving towards industry 4.0 whereby university 4.0 is also part of the movement.

- Since information security scholars argued that the types and strategies of ISC are slightly different according to size and type of the organization (Ayyagari & Tyks, 2012; Dojkovski et al., 2007b; Kuusisto & Ilvonen, 2003; Lopes & Oliveira, 2014; Main, Ky, Dixie, Al-Hamdani, & Dixie, 2009; Williams, 2009b), this research provides ISC model that could be used by public universities or any similar organizational settings in planning and implementing effective ISC to increase ISP compliance. These are crucial because they require guidance in establishing an information security-aware or implementing an acceptable ISC (Da Veiga & Eloff, 2010).

- The findings would provide new knowledge applicable to Malaysian employees because according to certain studies, information security behavior and ISC depend on national culture (Hovav & D'Arcy, 2012; Rocha Flores, Antonsen, & Ekstedt, 2014 Connolly & Lang, 2013; Govender, Kritzinger, & Loock, 2016).

1.7 Structure of the Thesis

The current chapter introduces the context of research, which cover issues of background, problem statement, gaps, research questions and objectives as well as research significance in order to give an overview of this research. To explain further insight pertaining to the study, the remaining chapters of the thesis are as follow:

Chapter 2: The literature review chapter discusses previous studies in the areas of ISC and ISP compliance behavior in great detail. It provides clear picture of the current status of all related issues pertaining to this study including identifying and analyzing research gaps that contribute to research problems and research questions. It also identifying the theories and concepts for the development of ISC model for ISP compliance behavior.

Chapter 3: The research model and hypotheses development chapter explains about theoretical framework of the study. It also describes the conceptual framework developed in this research and discusses the development of hypotheses.

Chapter 4: The methodology chapter elaborates on research paradigm and research operational framework employed in this research. This chapter also discusses the population, sampling size, data collection procedures as well as data processing and analysis used in this research.

Chapter 5: Research instrument development chapter describes the processes involve in the development of survey questionnaire to collect data. This chapter also discusses the pre-tests and pilot studies conducted to test and improve the research instrument.

Chapter 6: The findings and discussions chapter analyzes the data as well as presents and discusses the findings of the statistical analysis of data using Partial Least Square Structural Equation Modelling (PLS-SEM) technique.

Chapter 7: The conclusions chapter concludes all findings based on research questions and research objectives of the study. This chapter also suggests the contributions and implications, describes the limitations of the research as well as offers suggestions for future researches.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Information Security Culture (ISC) is recommended by scholars as an effective strategy in guiding security behavior among employees in organization. Interestingly, the most desired employees' behavior is to follow Information Security Policy (ISP) established in the organization. Therefore, these two important concepts complement each other and highly demanded in many organizations. This chapter reviews and discusses related studies in these two areas. The main objective is to analyze current findings and to identify the gaps, theories and concepts to develop ISC model for ISP compliance behavior.

Figure 2.1 shows the main structure of review in this chapter. It has four areas with the main focus is on ISC and ISP compliance behavior. The purpose of review on ISC literature is to analyze ISC concepts, models and frameworks in order to identify current findings as well as gaps in terms of factors, dimensions and theories used to conceptualize ISC. As depicted in the figure, the findings for this particular review are used to formulate dimensions of ISC concept employed in this research.

As for ISP compliance behavior, the review was performed to analyze how ISP compliance studies were conducted in order to determine the patterns employed in ISP compliance behavior models. These include review and analysis on theories, factors, dependent variables and findings to identify the most significant themes to be considered for this research. The key issues, theories and factors were identified to create the conceptual relationship between ISC and ISP compliance behavior.

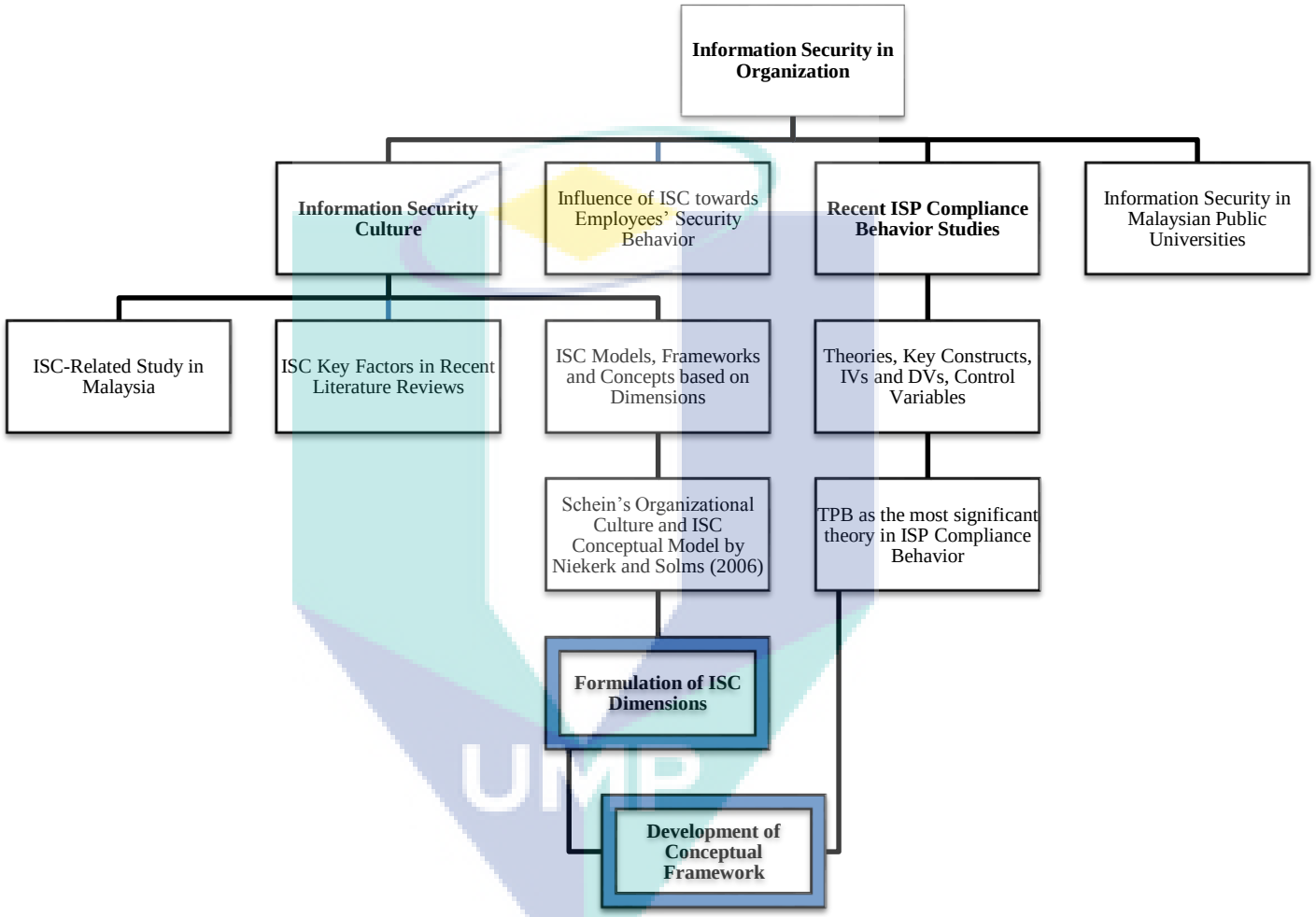


Figure 2.1 Main Structure of Literature Review

The chapter also reviews about information security issues, ISC and ISP compliance behavior studies in the context of Malaysian organization to identify the latest issues and development in these two areas. Additionally, since this study focuses on Higher Educational Institutions (HEIs) sector particularly public universities, review about information security in this sector is also included. This chapter concludes with summary of key findings that directed to the justification for developing and validating a new ISC model based on dimensions for employees' ISP compliance behavior in Malaysian public universities.

2.2 Information Security in the Organization

Information within the organization has become important asset that can create significant competitive advantage; therefore, needs to be protected. Information security can be defined as the protection of information systems from unauthorized access and information threat (Rhee, Kim, & Ryu, 2009). Information security in the organization must be implemented to ensure the confidentiality, integrity and availability of the information (Chang et al., 2007). Normal practice for information security provision is the implementation of technological solutions such as installing firewalls, updating anti-virus software, backing up the systems, maintaining and restricting access controls, using encryption keys, using surge protectors, and using comprehensive monitoring systems (Lee & Larsen, 2009; Ryan, 2004; Workman et al., 2008). These technical solutions are effective to combat breaches or attacks from hackers outside the organization. Although these solutions help improve information security, relying on them alone is insufficient to eliminate risk (Bulgurcu, Cavusoglu, & Benbasat, 2010a) and to provide total protection for Information System (IS) organizational resources (Herath & Rao, 2009b; Rhodes, 2001; Sasse et al., 2004; Stanton et al., 2005). Experts believe that the technology aspects of information security cannot solely guarantee a secure environment (Safa, Von Solms, & Furnell, 2016) and that human information security behavior should be taken into consideration (Cram et al., 2017; Furnell & Clarke, 2012; Tang et al., 2016). This is due to the fact that the organization not only needs to be protected from "known outside attackers", but also needs to be protected from their own employees inside the organization.

In the context of information security, employees are also considered as attackers alongside with other profiles such as hackers, crackers, script-kiddies and

cyber-terrorist (Ciampa, 2012). The employees are the people inside the organizations that know more information, closer to the target and lesser security mechanisms applied compared to other profile of attackers (Schultz, 2002; Willison & Siponen, 2009). Realistically, these facts are terrifying for employers; as employees are the weakest link in information security in any organization (Hu, Dinev, Hart, & Cooke, 2012; Mahfuth et al., 2017; Vroom & Von Solms, 2004; Warkentin & Willison, 2009). In fact, a large number of security breaches caused by insider breach and internal employee negligence (Chen et al., 2015). Most of the occurrences are due to their behaviors and practices upon dealing with information assets in the organization (Baker et al., 2010; Boujettif & Wang, 2010; Kathryn et al., 2017; Poll, 2015; PWC, 2015; Richardson, 2011; Thomson, Von Solms, & Louw, 2006). The literature shows that majority of security incidents are caused by trusted employees who fail to follow ISP in dealing with information assets (Fagade & Tryfonas, 2017; Ifinedo, 2016; PWC, 2008; Vroom & Von Solms, 2004; Whitman, 2008). Various reports and studies suggest employees as the biggest threat to worldwide organizations' information security (Bulgurcu et al., 2010a; Crossler et al., 2012; Robert, 2011; Durbin, 2016; Thomson et al., 2006; Verizon Business, 2011; Von Solms, 2000) including Malaysia (CyberSecurity Malaysia, 2015). In addition, employees are hackers' popular targets to intrude into organization's network and information systems by exploiting their weaknesses into performing actions benefiting the hackers (Flores & Ekstedt, 2016). It was estimated that around 20 per cent of employees enter their usernames and passwords in response to faked "phishing" e-mails, which pretend to originate from legitimate sources (Economist, 2014).

Recent trend of attacks and breaches such as Ransomware (The Hacker News, 2017a; The Sun Daily, 2017; Wiser.my, 2017) proved that security responsibility and causes of security holes are not on the technology but the people. The latest Ransomware attacks considered as the biggest and damaging cyberattack in history (CNN tech, 2017; The Telegraph, 2017) demonstrate people's behavior and practices in dealing with information assets are the contributing factors causing the attack rather than the technology such as firewall or anti-virus. Reports and experts claimed the attack exploits the vulnerabilities in computer systems caused by system administrators and users who fail to apply proper security procedure such as making regular updates and patches (The Hacker News, 2017a, 2017b). Following the attacks, experts suggested for employees to strictly follow security requirement documented in ISP to

minimize the threats (Cyber Security Malaysia, 2017). Unfortunately, employees' ISP compliance issue is still unresolved and remains to gain attention from researchers in order to understand and overcome the issue. More often than not, employees fail to realize security consequences of their actions and fail to understand the impacts of their security decision (Zurko, Kaufman, Spanbauer, & Bassett, 2002). Normally, this situation caused by organizational culture pertaining to the importance of information security.

In order to provide more comprehensive solution to information security in an organization, employees' behavior in dealing with information assets needs to be considered because information security depends on human effective behavior (Siponen, 2005; Stanton et al., 2004, 2005; Von Solms & Von Solms, 2004; Vroom & Von Solms, 2004; Workman, 2007). Although many organizations invest in the technological aspects of information security and tools, number of security incidents and breaches continue to be significant problem due to the lack of attention to employees in organizations (Glaspie & Karwowski, 2018; Ifinedo, 2012). According to Kolkowska (2011), information security is viewed from socio-organizational perspective and the literature in this field emphasizes that employees' behaviors, values and beliefs must be addressed in order to protect the information assets (Siponen 2005; Mishra & Dhillon 2006; Dhillon 2007).

Information Security Management (ISM) of any organization should implement a more integrated approach by cultivating a culture of information security (Lopes & Oliveira, 2014; Williams, 2009b) in guiding employees' behavior as documented in organization's ISP (Cox, 2012; Alfawaz et al., 2010; Vroom & Von Solms, 2004). By cultivating Information Security Culture (ISC), besides implementing and focusing technological aspects, the organization could also focus in improving human aspects in terms of employees' security behavior and practices. According to Lopes and Oliveira (2014), "one cannot talk about information security in an organization without addressing and understanding the ISC of that institution". Previous studies indicate that organizations that have neglected to focus on individuals fail to achieve success in their efforts (Li, Zhang, & Sarathy, 2010; Stanton et al., 2005a; Webb, Ahmad, Maynard, & Shanks, 2014).

2.3 Information Security Culture and Its Relationship with Information Security Policy Compliance Behavior

Many definitions of Information Security Culture (ISC) were identified in the literature. Ngo, Zhou, and Warren (2005) refers ISC as accepted actions and behaviour of employees in regards to information security in the organization. Mcllwraith (2006) defines ISC as individual employee's belief on the value of complying with information security standards and policies. Malcolmson (2009) suggested that ISC to emerge from employees' assumptions, attitudes, values, beliefs and behaviour, which can affect the information security of an organisation. Da Veiga and Eloff (2010) proposed that ISC changes over time and it is about employees' assumptions, attitudes, beliefs, values and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time. The most recent definition available by Alhogail and Mirza (2014b) refers ISC as the collection of perceptions, attitudes, values, assumptions, and knowledge that guide human interaction with information assets in an organization with the aim of influencing employees' behavior to preserve information security.

Clearly, all definitions above refer ISC as employees' behavior, attitudes, values perceptions, attitude and all other cognitive elements to form a culture that emphasizes on the security of information assets by improving employees' information security behavior. It is a culture that promotes security behavior and thus contributes to achieving the overall goals of the organization (Bozic, 2012). This culture "consists of a shared pattern of values, mental models and activities that are traded among an organization's employees over time, affecting information security" (Karlsson et al., 2015). A security culture could be engendered "by instilling the aspects of information security to every employee as a natural way of performing his or her daily job" (Oost & Chew, 2007). It includes all socio-cultural measures supporting technical security methods, so that information security becomes a natural aspect in the daily activity of every employee (Schlienger & Teufel, 2003b).

Since many researchers and experts believe information security is both "people issue" and "technical issue" (Schultz, 2005), ISC is the answer in bridging and complementing each other. Von Solms (2006) noted that various information security controls could only be managed properly if a comprehensive ISC is in place, whereby

the employees know, understand, and accept the necessary precautions. Furthermore, ISC is widely accepted as an effective mechanism to manage human factor particularly in guiding employees' information security behavior (Da Veiga & Eloff, 2010; Lim et al., 2009; Van Niekerk & Von Solms, 2010; Williams, 2009b). The establishment and implementation of ISC promote the improvement in information security practice (Alfawaz et al., 2010; Williams, 2009b) and improve ISP compliance (Alfawaz et al., 2010; Vroom & Von Solms, 2004) as security behaviors become second nature to employees (Thomson et al., 2006). Scholars also claim ISC would reduce security incident and minimize information security risks (Baggett, 2003; Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015b; Drevin, Kruger, & Steyn, 2007; ISF, 2000; Martins & Eloff, 2002; Schlienger & Teufel, 2005; Shahibi et al., 2012; Von Solms, 2006; Zakaria, 2006).

The aforementioned arguments lead to the fact that ISC would influence and improve employees' information security behavior. Padayachee (2012) has defined security behavior as a set of core information security activities that have to be adhered by end-users to maintain information security as defined by ISP. From this perspective, the implementation of ISC would influence and improve employees' behaviors towards ISP compliance in the organization. In fact, ISC and ISP compliance behavior are related and overlapped one another. ISC is frequently linked to employees' security behavior and this fact was discussed by Vroom and Von Solms (2004). They recommended ISC as an approach to improve employees' ISP compliance behavior and argued that ISC could be assessed by examining employees' security behavior. This is also the reason for Sherif and Furnell (2015) to develop ISC cultivation model, whereby the key variables of both ISP compliance behavior and ISC are applied as the key elements in building their model. Other study such as Tang et al. (2016) have directly assumed that information security behavior could be referred as ISC.

Based on aforementioned discussions, since scholars said that ISC would influence employees' information security behavior; and this behavior is related to the behavior that in line with ISP; therefore, it could be concluded that ISC is a collection of beliefs, values, behavior, assumptions, practices, attitudes and knowledge regarding information security that would influence employees' information security behavior,

particularly in adhering to ISP established in the organization, as illustrated in Figure 2.2.

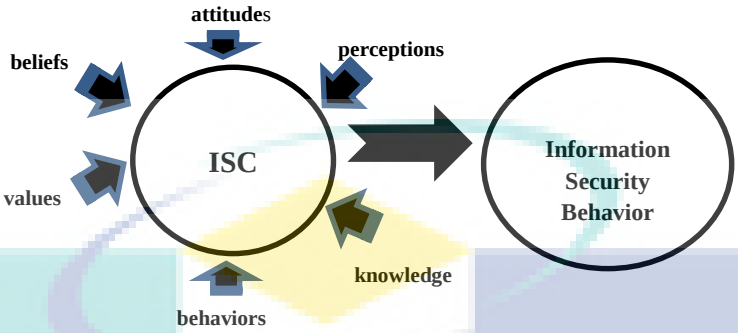


Figure 2.2 ISC and Information Security Behavior

2.4 ISC Factor and ISC Dimension

Generally, the terms factor and dimension are used interchangeably in ISC literature. Some authors use factors; while, some others use dimensions in referring to the element and aspect of ISC concept. For example Top Management Commitment is called a dimension in Temesgen, Lessa, and Ferede (2011); whereas it is referred to as a factor in Alnatheer (2014). Another example is ISP Enforcement which is referred to as dimension in Hassan et al. (2017) and as a factor in Alnatheer (2014). Meanwhile, some authors used subdimension instead of factor such as Martins and Eloff (2002).

Nevertheless, most authors preferred the term dimension instead of factor when discussing ISC models and frameworks such as Da Veiga (2016); Martins and Da Veiga (2014b); Da Veiga (2015b). The term factor is utilized to explain a single overlapped ISC element; whereas the dimension is employed to represent a distinct aspect containing a group of several factors. For example, the conceptual model by Zakaria and Gani (2003) consists of three dimensions; whereby, each dimension contains several relevant factors (Dojkovski, Lichtenstein, & Warren, 2007c). Based on these facts and arguments, this thesis also using the same representation and definition of dimension and factor by Zakaria and Gani (2003). As shown in Table 2.1, a factor is an element of ISC whereas a dimension is a distint aspect of ISC that contain several similar factors in it.

In discussing ISC from the context of Organizational Culture (OC), most authors used the terms dimension rather than factor. For example, ISC framework by

Ruighaver, Maynard, and Chang (2007) used the term dimension (Oost & Chew, 2007) in conceptualizing ISC as direct representation for dimensions in OC by Detert et al. (2000). This is also the same case in ISC framework by Van Niekerk and Von Solms (2006) who applied the term of dimension (Reid et al., 2014) for each ISC level conceptualized based on OC by Schein (1992). Recently, the term dimension has been widely used by authors who study ISCA such as in Da Veiga (2016); Martins and Da Veiga (2014b); Da Veiga (2015b). Therefore, the dimension is more appropriate in discussing ISC because ISC is a subculture of OC.

Table 2.1 Factor and Dimension Context

Term	Definition	Example
Factor	a single element of ISC	Information Security Policy, Ethical Conduct Policy
Dimension	a distinct aspect containing a group of several similar factors/element	Procedural Countermeasures

2.5 ISC Models, Frameworks and Concepts based on Dimensions in Literature

As discussed in Section 2.4, the term dimension is a more common used in discussing ISC concept or model. In fact, the term dimension is more appropriate to be referred in discussing about culture. Since this thesis is all about the concept and model of ISC, the term factor is used from this section on to represent a single overlapped ISC element; whereas, the term dimension is used to represent a distinct ISC aspect that groups several relevant factors together.

A systematic literature review was conducted to analyze all the possible ISC concept based on dimension available in the literature. Eight leading electronic databases were selected for identifying potential articles: Scopus, Web of Science, Google scholar, IEEE/IEE Electronic Library, EBSCOhost, ACM Digital Library, Elsevier Science Direct, and Emerald Library. Search was conducted using keywords of "information security culture" and "security culture". The search included journals and conference articles as well as Masters and PhD thesis published during the period of 2000 to 2017. Figure 2.3 shows the flow diagram regarding the systematic search, inclusion and exclusion of studies in this review.

A total of 405 articles was extracted based on the search strategy. After removing duplicated papers, 239 potential articles remained. Titles and abstracts were then screened and irrelevant studies were removed, cutting down the potential articles to 205.

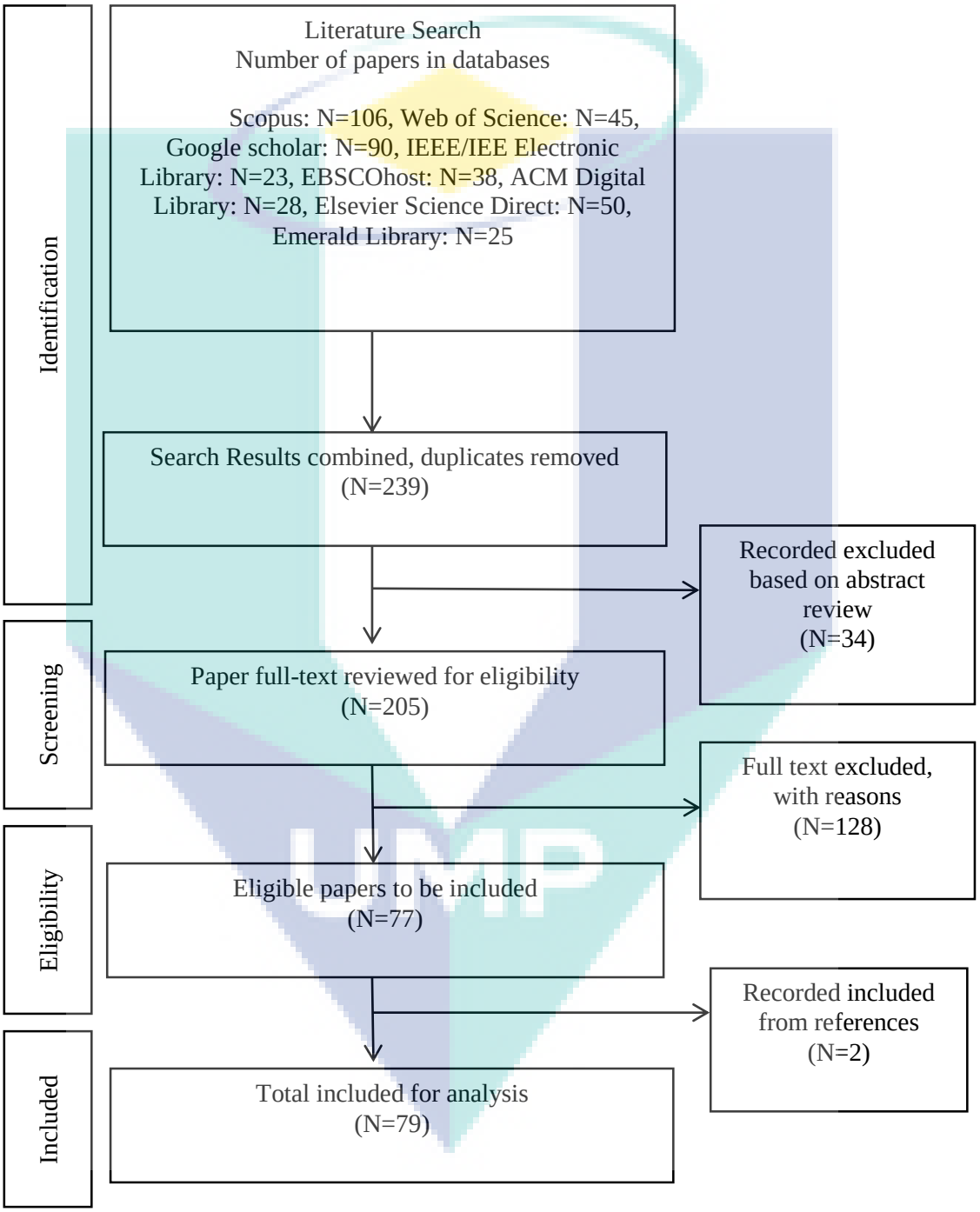


Figure 2.3 Flow diagram regarding the systematic search, inclusion and exclusion of studies

2.5.1 Study Selection and Eligible Papers

The remaining 205 full-text articles were reviewed and analyzed for eligibility. These articles consist of studies on ISC models and concepts in organizational settings. The dimensions used in ISC were carefully identified as some articles did not explicitly mention the dimensions employed. In some articles, dimensions were referred to as "factor". Some papers used dimensions in discussing ISC cultivation and some papers refer them for improving current ISC in the organization. Interestingly, some papers such as Da Veiga and Eloff (2010); Martins and Eloff (2002); and Tolah, Furnell, and Papadaki (2017) used both terms of cultivating (e.g. create, implement) and managing (e.g. assess, improve) in discussing the ISC concept in their papers. Therefore, as long as the factors fit the definition of dimensions, the articles were selected for further analysis.

Articles that did not discuss the dimensions of ISC were excluded. In addition, articles that discussed ISC in other settings such as smart living environment were also excluded from this review. Articles that discussed Information Security Climate, Information Security Obedience or Information Security Management without focusing on any ISC model or concepts were excluded as well. Two studies by Nenad (2013) and Cárdenas-Solano, Martínez-Ardila, and Becerra-Ardila (2016) were excluded since the English version of the paper were not available. A study by Mcintosh (2011) too was excluded because the full version of the article could not be downloaded. Two more papers identified from the references of the selected papers also included since these papers met the selection criteria. The final number of eligible articles was 79 as depicted in Figure 2.3.

2.5.2 Data Extraction and Summary

Each article was categorized based on ISC concept and its dimensions. All dimensions were recorded in a single column as depicted in Table 2.2. Some articles also discussed subdimensions of ISC and were recorded in the same column. The concepts, theories and approaches adopted in conceptualizing ISC were recorded in the last column.

In general, it was found that it is a common practice to use more than a single theory in the conceptualization of ISC. For example, ISC concept by Schlienger and

Teufel (2002) is based on Organization Culture concept by Schein (1992) and Corporate Culture concept by Rühli (1991). There are also a number of articles that solely used literature review to identify the dimensions of ISC. Some articles used both literature review and theory to model ISC. All these approaches were recorded for further analysis. Table 2.2 clearly indicates that there are various concepts of ISC based on different different sets of dimension. Generally, at least 47 variances of ISC concepts based on dimensions have been identified in the studies reviewed.

2.5.3 Theories and Concept Adopted in ISC Model

Although Table 2.2 shows that theories, concepts and approaches are one of the main factors that contribute to the differences in ISC dimensions, other possible factors might play some significant role towards this issue. The following sub-sections discuss the issue by classifying the concepts, theories and other factors contributing to the differences in ISC dimensions.

2.5.3.1 ISC Based on Organizational Culture

Majority of earlier ISC studies adopted the concepts of Organizational Culture (OC) and Organizational Behavior (OB) in ISC conceptualization. This is not a new finding since Alhogail and Mirza (2014) and Pevchikh (2015) had acknowledged this fact in their review. Besides the popularity of OC concept by Schein (1985, 1992, 1999), OC concept by Detert et al. (2000) is also used as a point of reference in constructing ISC model. These two concepts are different; thus, ISC dimensions and factors derived from these two concepts are also different.

As shown in Table 2.2, besides based on literature review, majority of studies used Schein's OC concept to conceptualize their ISC compared to other concepts. ISC developed based on this concept basically has three dimensions representing the three levels of OC, namely Artifacts; Espoused values; and Basic assumptions and beliefs. Among the ISC models adapting this Schein's OC are Da Veiga and Eloff (2010); Schlienger and Teufel (2003a) as shown in Figure 2.4. Nevertheless, there is no similarity in terms of subdimensions or factors used in all these ISC models. For example, Schlienger and Teufel (2002) used three dimensions, which are Corporate politics, Management, and Individuals with eleven factors/subdimensions associated with the dimensions.

Meanwhile, Chen et al. (2015) directly used three dimensions of Security Policy; Security Education, Training and Awareness (SETA); and Computer Monitoring to represent two out of three OC levels by Schein. These differences are also noticeable in other ISC models from the studies adopting Schein's OC. The most relevant explanation for this is that, in those studies, instead of using Schein's OC, they were also considered other concepts, such as Organizational Behavior and Information Security Components as evidenced in Martins and Da Veiga (2015a); Da Veiga and Martins (2015a); and Da Veiga and Eloff (2010) or Organizational Climate, Rewards and Punishments in Parsons et al. (2015).

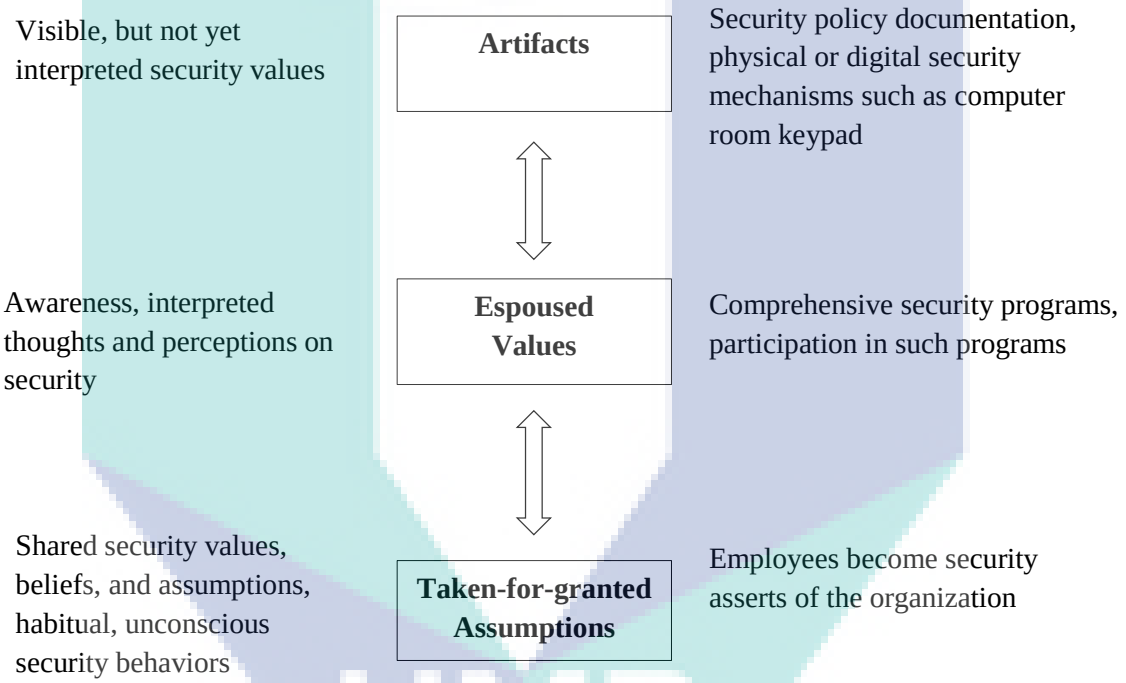


Figure 2.4 ISC model based on Schein's OC in Da Veiga and Eloff (2010); Schlienger and Teufel (2003a)

Source: Chen et al. (2015)

There are also ISC models which solely used the levels of Schein's OC without additional concepts such as in studies by Van Niekerk and Von Solms (2005, 2006, 2010). Another recent ISC model that embraced the Schein's OC concept can be found in a series of study by a group of researchers developing an instrument of ISC assessment (ISCA) such as by Da Veiga and Martins (2015a); Martins and Da Veiga (2015b); and Da Veiga (2015).

Table 2.2 ISC Concept Based on Dimensions and Approaches

No.	Author	Dimensions and Subdimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
1.	Schlienger & Teufel (2002)	**3 Dimensions**: Corporate Politics, Management, Individuals **11 Subdimensions**: Security Policy, Organizational Structure, Resources, Implementation of Security Policy, Definition of Responsibilities, Qualification and Training, Awards and Prosecutions, Audit and benchmarks, Critical Attitude, Act carefully and with due diligence, Communication	• Organizational Culture (Schein, 1992, 1999) • Corporate Culture (Rühli, 1991)
2.	Van Niekerk & Von Solms (2005), Van Niekerk & Von Solms (2010), Van Niekerk & Von Solms (2006), Van Niekerk (2005a), Reid & Van Niekerk (2014), Reid et al., (2014), Van Niekerk & Von Solms (2013)	**4 Dimensions**: Artifacts, espoused values, shared tacit assumptions, information security knowledge **4 Subdimensions**/Factors: ISP, Security Knowledge, Belief, Security Behavior	• Organizational Culture (Schein, 1992, 1999)
3.	Da Veiga & Eloff (2010)	**7 Dimensions**: Leadership and Governance, Security Management and Operations, Security Policies, Security Program Management, User Security Management, Technology Protection and Operations, Change Management	• Organizational Culture (Schein, 1992, 1999) • Organizational Behavior (Robbins, Odendaal, & Roodt, 2003) • Information Security Components (Da Veiga & Eloff, 2007)
4.	Da Veiga & Martins (2015a), Martins & Da Veiga (2015b), Da Veiga (2015), Da Veiga (2015a)	**9 Dimensions**: Information Asset Management, Information Security Management, Change Management, User Management, Information Security Policies, Information Security Program, Trust, Information Security Leadership, Training and Awareness	• Organizational Culture (Schein, 1992, 1999) • Organizational Behavior (Robbins et al., 2003) Information Security Components by Da Veiga and Eloff (2007), using dimensions similar to Da Veiga, Martins, and Eloff (2007)

Table 2.2 continued

No.	Author	Dimensions and Subdimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
4.	Da Veiga & Martins (2015a), Martins & Da Veiga (2015b), Da Veiga (2015), Da Veiga (2015a)	**9 Dimensions**: Information Asset Management, Information Security Management, Change Management, User Management, Information Security Policies, Information Security Program, Trust, Information Security Leadership, Training and Awareness	• Organizational Culture (Schein, 1992, 1999) • Organizational Behavior (Robbins et al., 2003) • Information Security Components by Da Veiga and Eloff (2007), using dimensions similar to Da Veiga, Martins, and Eloff (2007)
5.	Martins & Da Veiga (2015)	**4 Dimensions**: Management, Policies, Awareness, Compliance **9 Subdimensions**: Information Security Commitment, Information Security Importance, Information Security Policy Effectiveness, Information Security Directives, Information Security Responsibility, Information Security Necessity, Information Security Assets, Information Security Monitoring Perception, Information Security Consequences	• Organizational Culture (Schein, 1992, 1999) • Organizational Behavior (Robbins et al., 2003) • Information Security Components by Da Veiga and Eloff (2007) • Literature Review
6.	Chen et al. (2015)	**3 Dimensions**: Artifacts and creations, Collective Values, Norms and Knowledge, Basic assumptions and beliefs **3 Subdimensions**: Security Policy, SETA, Computer Monitoring	• Organizational Culture (Schein, 1992, 1999) • ISC Conceptual Model (Van Niekerk & Von Solms, 2006, 2010)
7.	Parsons et al. (2015)	**4 Dimensions**: Sanctions, Rewards, Job Roles, No. of Employee	• Organizational Culture (Schein, 1992, 1999) • Organizational climate, rewards and punishments
8.	Kraemer & Carayon (2005)	**6 Dimensions**: Employee Participation, Training, Hiring Practices, Reward System, Management Commitment, Communication and Feedback	• Organizational Culture (Schein, 1992, 1999) • Organizational Culture by Guldenmund (2000)

Table 2.2 continued

No.	Author	Dimensions and Subdimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
9.	Hassan et al. (2017)	**12 Dimensions**: Security Knowledge; Security Awareness; Security Behavior; Security Policy Enforcement; Security Decision Making Should Rely On Facts And Rationality That Security Is Important; Improving Information Security Requires A Long-Term Commitment; Proper Security Systems And Process Motivate Employee To Adhere To Security Policies And Procedure; Organizations Must Make Continuous Changes To Improve Information Security; Employee Should Be Involved In Improving The Overall Organization's Information Security; Collaboration And Cooperation Are Necessary For Effective Information Security; A Shared Security Vision And Shared Security Goals Are Critical For Effective Information Security; Information Security Needs Should Be Determined By External And Internal Requirements; Top Management Commitment	• Organizational Culture (Schein, 1992, 1999) • Health Belief Model (HBM) • Literature review
10.	Chia et al. (2003a), Ruighaver et al. (2007), Chia et al. (2002a, 2002b), Parsons et al. (2010), Koh et al. (2005)	**8 Dimensions**: The Basis of Truth and Rationality; The Nature of Time and Time Horizon; Motivation; Stability versus Change/Innovation/Personal Growth; Orientation to Work, Task, Co-Workers; Isolation versus Collaboration/Cooperation; Control, Coordination and Responsibility; Orientation and Focus – Internal and/or External **11 Subdimensions**: Belief of The Importance of Security, Trust, Security Goals, Security Strategies, Social Participation, Change Management, Responsible for Security, Employee's Involvement in Security and Collaboration, Top Management Commitment, Security Governance, External Factors and Internal Need	• Organizational Culture (Detert, Schroeder, & Mauriel, 2000)
11.	Ramachandran et al. (2008), Ramachandran et al. (2013)	**3 Dimensions**: Beliefs about identity, Beliefs about rule compliance, and Beliefs about security	• Organizational Culture (Detert et al., 2000) • ISC Framework by Tejay & Dhillon (2005), Chia et al. (2002b)

Table 2.2 continued

No.	Author	Dimensions and Subdimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
12.	Lim et al. (2010), Lim et al. (2009)	**8 Dimensions**: The Basis of Truth and Rationality; The Nature of Time and Time Horizon; Motivation; Stability versus Change/Innovation/Personal Growth; Orientation to Work, Task, Co-Workers; Isolation versus Collaboration/Cooperation; Control, Coordination and Responsibility; Orientation and Focus – Internal and/or External **5 Subdimensions**: Management involvement, locus of responsibility, information security policy, education/training, budget practice	• Organizational Culture (Detert et al., 2000)
13.	Tang et al. (2016)	**4 Dimensions**: Compliance, Communication, Accountability, Governance	• Hofstede's organizational culture framework (Hofstede, Neuijen, & Ohayv, 1990) • Information Technology Security Management (Werlinger, Hawkey, & Beznosov, 2009)
14.	Alhogail (2015b), Alhogail & Mirza (2014a), Alhogail (2015a), Alhogail & Mirza (2015), Alhogail & Mirza (2014a)	**9 Dimensions**: Strategy, Technology, Organizational, People, Environment, Preparedness, Responsibility, Management, Society and Regulations **10 Subdimensions**: Training, Focus groups, Change agents, Motivation, Milestones and measures, Involvement, Management support, Resources, Communications, Culture analysis	• ISC Conceptual Model (Van Niekerk & Von Solms, 2006, 2010) • STOPE (Bakry, 2003), Human Diamond Dimension and Change Management
15.	Da Veiga et al. (2007), Da Veiga (2008)	**8 Dimensions**: Information Asset Management, Information Security Management, Change Management, User Management, Information Security Policies, Information Security Program, Trust, Information Security Leadership ***6 Dimensions after factor and reliability analysis**: Management of Information Security, Performance Management, Performance Accountability, Communication, Governance, Capability Development	• Organizational Behavior (Robbins et al., 2003)

Table 2.2 continued

No.	Author	Dimensions and Subdimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
16.	Martins & Eloff (2002); Martins (2001)	**9 Dimensions**: Policy and Procedures, Risk analysis, Benchmarking, Budget, Management, Trust, Awareness, Ethical Conduct, Change	• Organizational Behavior (Robbins et al., 2003) • Organizational Culture
17.	Martins & Da Veiga (2014)	**8 Dimensions**: Information Asset Management, Information Security Management, Change Management, User Management, Information Security Policies, Information Security Program, Trust, Information Security Leadership	• Organizational Behavior (Robbins et al., 2003)
18.	Da Veiga & Martins (2015b), Martins & Da Veiga (2010), Da Veiga & Martins (2017)	**10 Dimensions**: Information Asset Management, Information Security Management, Change Management, User Management, Information Security Policies, Information Security Program, Trust, Information Security Leadership, Training and Awareness, Privacy Perception ***6 Dimensions after factor and reliability analysis**: Information Security Commitment, Management Buy- in, Information Security Necessity and Importance, Information Security Policy Effectiveness, Information Security Accountability, Information Usage Perception	• Organizational Behavior (Robbins et al., 2003) *Same dimension with Martins & Da Veiga (2014) but with two added dimensions of Training and Awareness, Privacy Perception
19.	Helokunnas & Kuusisto (2003)	**3 Dimensions**: Technical, Management and Institutional Wave	• Information Security Awareness by Siponen (2000)
20.	Kuusisto et al. (2004)	**5 Dimensions**: Resources, Security policy, Commonly accepted norms, The unity of values of all parties involved to security culture forming process, The communication distance.	• Habermas' theory of communicative action (Habermas, 1984, 1989)
21.	Knapp et al. (2006)	**1 Dimension**: Top management	• Analyze open-ended questions • Literature review
22.	Dhillon et al. (2016)	**10 Dimensions**: Interaction, Association, Subsistence, Bisexuality, Territoriality, Temporality, Learning, Recreation and Humor, Defense, Exploitation	• Hall's theory of cultural messages (Hall, 1959)

Table 2.2 continued

No.	Author	Dimensions and Subdimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
23.	Alfawaz et al. (2010)	**3 Dimensions**: Knowledge, Skills, and Individual Preferences Work	• Literature review • Utilizing "knowing-doing gap" concept by Pfeffer & Sutton (2000), Classification Theory by Smith & Medin (1981) and Parsons (1996)
24.	Alfawaz (2011)	**3 Dimensions**: Organizational culture, National culture, Technological **12 Subdimensions**: Top management commitment, IS structure, Skills and training, Awareness, Motivation, Information and knowledge sharing, Information security technology, Change management, Power distance, Individualism vs. collectivism, Uncertainty avoidance, Context	• National Culture by Hofstede (2001) • Context Culture Value by Hall (1976) • ISC Framework by Chia et al. (2002b)
25.	Baggett (2003), (I-WAYS, 2003)	**9 Dimensions**: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, Reassessment	• Guidelines for Security of Information Systems and Networks. • (OECD, 2002) of the Organization for Economic Cooperation and Development (OECD)
26.	Al-Mayahi & Mansoor (2013)	**3 Dimensions**: ISP, ISP Awareness, Compliance	• The process of full adoption of ISC in an organization by Chia, Maynard, & Ruighaver (2002)
27.	Sherif & Furnell (2015), Sherif, Furnell, & Clarke (2015)	**5 Dimensions**: Security behavior, Top Management, Security Awareness and Education, Security Policy, Security Acceptance	• Literature review on information security compliance and ISC •

Table 2.2 continued

No.	Author	Dimensions and Subdimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
28.	Lopes & Oliveira (2014)	**11 Dimensions**: Security Policy; Organization of Information Security; Asset Management; Human Resources Security; Physical and Environmental Security; Communications and Operations Management; Access Control; Information Systems Acquisition, Development and Maintenance; Information Security Incident Management; Business Continuity Management; and Compliance	• ISO IEC 27002:2005 (Standard, 2005)
29.	Ramachandran & Rao (2006)	**4 Dimensions**: Security-related Belief, Management Actions Emphasizing IS Security, Management Actions Emphasizing Productivity, Top Management Teams' Belief	• Literature review
30.	Williams (2009)	**4 Dimensions**: Response not Reaction, Responsibility, Community of Practice, Awareness **23 Subdimensions**: What is being protected; Value versus cost; Risk assessment; Balanced/suitable response to threats; Internal policy and procedure; Legal; Policy: Standards and best practice; Internal and external obligations and perceptions of data privacy, rights of patients, rights of staff; Governance; Ethics, beliefs and trust; Socialization of the group; Capability; Adaptability to change; Management of security in organization; Information system used; Workflow integration; Risk perception; Security issues; Impact; Objectives of security; Breach identification and consequences; Personal motivation	• Literature review
31.	Alnatheer & Nelson (2009)	**4 Dimensions**: Corporate Citizenship, Legal Regulatory Environment, Corporate Governance, Cultural Factors	• Literature review
32.	M. Shahibi et al. (2012)	**4 Dimensions**: Principles, Organizational Behavior Tier, Culture Level, Security Control	• Literature review

Table 2.2 continued

No.	Author	Dimensions and Subdimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
33.	Hassan & Ismail (2012)	**6 Dimensions**: Behavioral, Change Management, Information Security Awareness, Organizational System, Security Requirements, Knowledge	• Literature review
34.	Alnatheer (2012), Alnatheer et al. (2012)	**3 Dimensions**: Top Management Involvement, Training, Policy Enforcement	• Literature review
35.	Alnatheer (2014)	**7 Dimensions**: Top Management Support, Security Policy and Policy Enforcement, Security Awareness, Security Training and Education, Security Risk Assessment, Security Compliance, Ethical Conduct	• Literature review
36.	Temesgen et al. (2011)	**5 Dimensions**: Knowledge to information security, Management of Information Security, Communication, Governance, Performance Accountability	• Literature review
37.	Dojkovski et al. (2006), Dojkovski et al. (2007a), Dojkovski et al. (2005)	**5 Dimensions**: Individual and Organizational Learning, E-learning, Managerial, Behavioral, Ethical, National and Organizational Culture **Subdimensions**: Policy and Procedures, Benchmarking, Risk Analysis, Budget, Management, Response, Training, Education, Awareness, Change Management, Responsibility, Integrity, Trust, Ethicality, Values, Motivation , Orientation, Personal Growth	• Literature review
38.	Dojkovski et al. (2007b), Dojkovski, Lichtenstein & Warren (2010)	**9 Dimensions**: Leadership/Corporate Governance, Organizational Culture, Managerial, Individual and Organizational Learning, Organizational Security Awareness, National and Ethical Culture, Government Initiatives, IT Vendors, Behavioral Issues **18 Subdimensions**: Risk Analysis, Budget, Policy and Procedures, Response, Self-Assessment, Employment contract/Handbook, E-learning, Training, Education, Informal Awareness, Marketing, Responsibility, Integrity, Trust, Ethicality, Values, Motivation , Orientation, Personal Growth	• Literature review
			•

Table 2.2 continued

No.	Author	Dimensions and Subdimensions/Factors (if any)	Adopted Theories, Concepts and/ or Approaches
39.	D'Arcy & Greene (2009)	**2 Dimensions**: Top Management Commitment, Security Communication	• Literature review
40.	D'Arcy & Greene (2014), Alharbi (2017)	**3 Dimensions**: Top Management Commitment, Security Communication, Computer Monitoring	• Literature review
41.	Alkalbani et al. (2015)	**3 Dimensions**: Top Management Commitment, Accountability, Information Security Awareness	• Literature review
42.	Greig et al. (2015)	**3 Dimensions**: ISP Awareness, Security Behavior, Information Security Knowledge	• Literature review
43.	Alnatheer (2015)	**8 Dimensions**: Top Management Support, ISP, Information Security Awareness, SETA, Information Security Risk Analysis and Assessment, Information Security Compliance, Ethical Conduct Policies, Organization Culture	• Literature review
44.	Hassan & Ismail (2016)	**4 Dimensions**: Security Behavior, Security Value, Security Awareness, Enforcement of Security Policy	• Literature review
45.	Tolah et al. (2017)	**7 Dimensions**: Top Management Support, ISP, Education and Training, Information Security Risk Assessment, Ethical Conduct, Job Satisfaction, Personality Traits	• Literature review
46.	Masrek (2017), Masrek, Nazrin Harun, & Khairulnizan Zaini (2017)	**6 Dimensions**: Management Support, Policy and Procedures, Compliance, Awareness, Budget and Technology	• Literature review
47.	Fagade & Tryfonas (2017)	**6 Dimensions**: Leadership and Governance, Security Management and Organizations, Security Policies, Security Program Management, User Security Management, Technology Protection and Operations	• Information Security Components (Da Veiga & Eloff, 2007)

On the other hand, there are a group of authors employing the OC concept by Detert et al. (2000) to model the ISC in their studies. As depicted in Table 2.2, ISC models adopting this concept have more dimensions compared to ISC concepts based on Schein's OC. ISC model conceptualized based on this concept comprises of eight dimensions, as described by Chia et al. (2003); Koh, Ruighaver, Maynard, and Ahmad (2005); and Ruighaver et al. (2007). They believed that OC by Detert et al. (2000) is useful and essential in explaining and understanding ISC concept. They believed and justified that ISC in every organization consisted of these eight dimensions and the differences are only in terms of strength or level of these dimensions but not according to the type of each organization. Specifically, in applying these eight dimensions, they discovered that Belief of the importance of security, Trust, Security goals, Security strategies, Social participation, Change management, Responsible for security, Employee's involvement in security and collaboration, Top management commitment, Security governance, External factors, and Internal need are the factors involved in ISC cultivation in an organization. Although there are slight differences in terms of factors or subdimensions used in these studies, the ISC dimensions are still similar.

It is also worth to note that although most of the studies are found to be directly adopted and influenced by these two OC concepts, there are also ISC concepts that referred to other OC such as by Hofstede et al. (1990) and Guldenmund (2000).

2.5.3.2 ISC Based on Model by Van Niekerk and Von Solms (2006, 2010)

Figure 2.5 shows ISC model by Van Niekerk & Von Solms (2006). As discussed in Section 2.5.3.1, their model is one of the models adapting the levels in Schein's OC. However, instead of using three levels in OC, they added another level, which is the information security knowledge as shown in Figure 2.6. They argued that this level is necessary to provide a stable ISC in the organization.

Besides being one of the most popular model employing Schein's OC, ISC model by Van Niekerk & Von Solms (2006) is also one of the most referred model in recent literature. For instance, in investigating the factors of ISC based on information security programs, Chen et al. (2015) referred to this model to conceptualize ISC in their study. Chen et al. (2015) proposed three factors, which are Security Policy, SETA, and Computer Monitoring and these factors are consistent with factors considered

earlier in previous ISC models based on Schein's OC (1999). Other recent ISC models were influenced by ISC model of Van Niekerk and Von Solms (2010) such as in the studies by Alhogail (2015a); Alhogail (2015b); Al Hogail and Mirza (2015). However, in these series of studies, ISC dimensions mostly are different from ISC model by Chen et al. (2015). The reason is instead of using conceptual model by Van Niekerk and Von Solms (2010), these studies also adopted other concepts such as STOPE (Strategy, Technology, Organization, People, and Environment) view (Bakry, 2003), Human Factor Diamond, and Change Management as shown in Table 2.2. However, one dimension found to be common in all these studies, which is Security Policy.

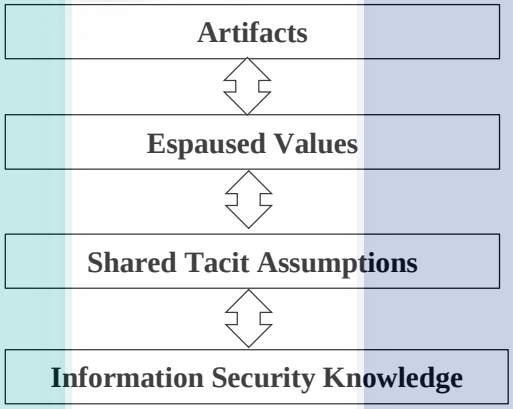


Figure 2.5 ISC model by Van Niekerk & Von Solms (2006)

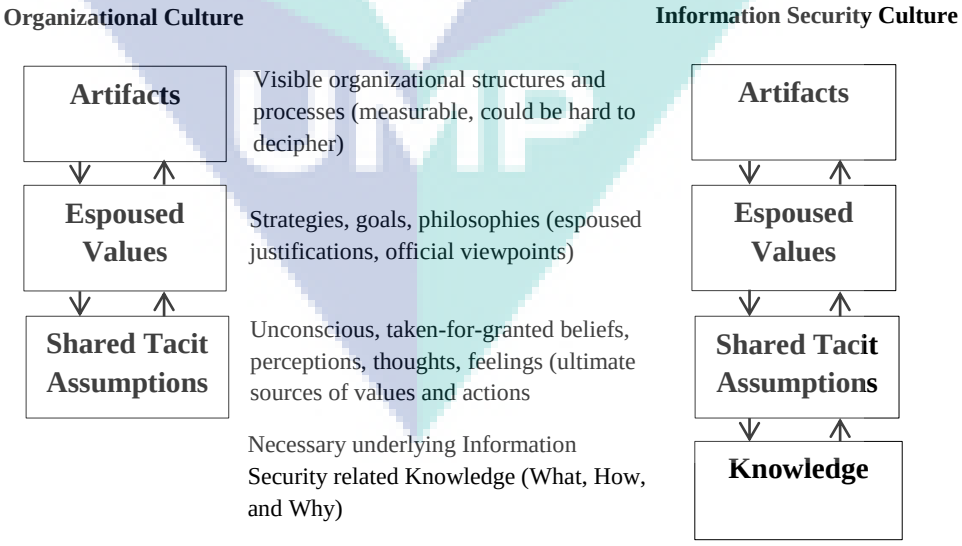


Figure 2.6 Adaption of Schein's OC in ISC model by Van Niekerk and Von Solms (2006)

2.5.3.3 ISC Based on Organizational Behavior

Despite the prevalent used of OC concept especially by Schein in ISC model, some researchers adopted Organizational Behavior (OB) concept by Robbins (2001) to construct ISC model. This concept is widely used in the development of Information Security Culture Assessment (ISCA). ISCA is a set of a questionnaire used to assess and evaluate the level and strength of ISC in an organization as well as to identify whether there is an adequate level of ISC in the organization. The questionnaire items were originally developed by Martins and Eloff (2002) based on OB by Robbins (2001). The model consists of three level components namely organizational, group, and individual and each level has its own ISC issues or dimensions. As shown in Figure 2.7, the dimensions of this ISC model are Policy and procedures, Risk analysis, Benchmarking, Budget, Management, Trust, Awareness, Ethical conduct and Change.

Figure 2.7 ISC Model by Martin and Eloff (2002)

This work then was continued by Da Veiga, Martins, and Eloff (2007) in their study to validate the instrument developed earlier by Martins and Eloff (2002). However, Da Veiga, Martins, and Eloff (2007) customized the instrument questionnaires based on a case study and eight new dimensions of ISC were introduced, namely ISP, Information security management, Information security program, Information security leadership, Information asset management, User management, Change management and Trust.

In relation to continuous development and validation of ISCA, Da Veiga and Eloff (2007) conducted a study to develop an information security governance framework. This framework comprised of seven dimensions including Leadership and Governance, Security Policies, Security Management and Organization, Security Program Management, User Security Management, Technology Protection and Operations, and Change Management. These dimensions were then used in a subsequent study by Da Veiga and Eloff (2010) to develop an ISC framework by integrating the concepts of Schein's OC (1985) and Robbins's OB (2001). This is the first study in which the authors formally named the framework as Information Security Culture Framework (ISCF) and this framework was widely used as the foundation of their next series of ISCA studies. ISCA instruments of ISC concept based on Da Veiga and Eloff (2010) and Da Veiga et al. (2007) were used widely in subsequent ISCA studies in Da Veiga and Martins (2015a, 2015b); Martins and Da Veiga (2014a, 2014b, 2015b). However, these studies did not use the same set of dimension in their ISC conceptualization. Again, as shown in Table 2.2, the reason is due to different additional concepts used instead of OB concept.

Specific objective of a study has some influences towards the differences in dimensions used. Interestingly, in regards to the ISCA-related studies, the authors explicitly mentioned that they customized the questionnaires from one study to another in order to meet specific type of organization under study (Da Veiga & Martins, 2015a, 2015b; Martins & Da Veiga, 2014a). According to Da Veiga and Martins (2015a), the changes in ISC questionnaires are due to the maturity level of information security of each organization under study such as ISP implementation and other information security programs. These questionnaires basically represented by particular constructs. Since the name of the construct changed, it seems that there is no finalized dimensions' set have been produced. This is not consistent with other authors, such as Chen et al. (2015) and Parsons et al. (2015) who used the same dimensions of ISC for all types of organization in their studies.

On the other hand, Martins and Da Veiga (2015b) had statistically proved that the same dimensions of ISCA can be applied to an international organizations operated in different countries that have different level of data protection maturity level. This fact suggests the same dimensions of ISC are applicable to similar type of organizations but

have different level of information security maturity. Interestingly, in reality, if similar type of organizations could have different maturity levels; then, different type of organizations might have different maturity levels. However, the authors did not mention the most appropriate or common dimensions of ISC concept applicable to all types of organization with different information security maturity level. This scenario suggest despite numerous ISCA-related studies producing validated assessment tools to measure and improve ISC of the organization under study, there is no mutual agreement on appropriate dimension to represent the ISC concept.

2.5.3.4 ISC Model from Information Security Culture Framework (ISCF)

The development and validation of ISCA influence the dimensions of ISC concept and initially started the development of Information Security Culture Framework (ISCF). The first ISCF was formally discussed by Da Veiga and Eloff (2010) and the framework was conceptualized in the form of interaction among the dimensions of Information Security Governance (Da Veiga & Eloff, 2007), the concept of OC (Schein, 1985) and OB (Robbins, 2001). However, recent studies by Alhogail (2015b), Alhogail (2015a), and Alhogail and Mirza (2015) have established a whole new concept of ISCF development. In this series of study, the authors developed and validated a comprehensive framework comprised of five dimensions of STOPE (Strategy, Technology, Organization, People, and Environment) and integrated with Change Management and Human Factor in information security. The framework also considered and used all levels of ISC model by Van Niekerk and Von Solms (2010) (Artifacts, Value, Belief and Information Security Knowledge). As a result, the dimensions of ISC once again consider different elements compared to previous studies of ISCA and ISCF.

2.5.3.5 Other Models

There are also other ISC models that were not developed based on certain theories or concepts, such as in Knapp et al. (2006); Alnatheer, Chan, and Nelson (2012); Shahibi et al. (2012); Alnatheer and Nelson (2009); Alnatheer (2014); Hassan and Ismail (2012); Dojkovski et al. (2010); and (Dojkovski et al., 2007b). These ISC models were developed based on literature analysis. Since most of the studies did not review similar articles, thus the dimensions produced were also different. For examples,

Sherif et al. (2015) identified five dimensions from 25 selected articles whilst Tolah et al. (2017) have identified 7 dimensions from 13 selected articles. Some studies combined both approaches of literature review and adopted particular concepts in modeling ISC such as by Knapp et al. (2006); Hassan et al. (2017); Martins and Da Veiga (2015); and Alfawaz et al. (2010). These studies also produced varied ISC dimensions as different concepts were used.

2.6 Conclusion on ISC Concept based on Dimension

As discussed in Section 2.5.3 and its sub-sections, there are various set of dimensions exist in modeling the ISC. While the concepts or theories adopted in conceptualized ISC play significant role on these differences, other factors such as specific objectives of the studies, approach taken by a study, the type of organization under study, and the maturity level of an organization's information security also contribute to this issue. Although there are some dimensions were consistently used in most of the studies such as Policy and Top Management Commitment, however, there are still too many differences in terms of number and name used to model ISC.

Moreover, there are some issues on the consistency of dimensions used throughout these studies. Some dimensions have different meanings even though they used similar term; for instance, the dimension of Trust. In Martins and Eloff (2002) and Da Veiga et al. (2007), Trust is defined as the "level of trust between employees and managers", whereas, in Da Veiga and Martins (2015b); Martins and Da Veiga (2010), it is defined as the "perceptions of users regarding the safekeeping of private information and their trust in the communications of the organization".

Some dimensions are found to have inconsistent name throughout these series of studies. For example, the dimension name of Security Management and Operations in Da Veiga and Eloff (2010) is called Security Management and Organization in Da Veiga and Eloff (2007) and these two names are referring to the same definition in both studies. Furthermore, in several studies, such as Da Veiga et al. (2007); Da Veiga and Martins (2015b); Martins and Da Veiga (2014b), some of the dimensions were changed after the factor and reliability analysis was performed, as shown in Table 2.2. For instance, the eight dimensions in a study by Da Veiga et al. (2007) were changed to six new dimensions' name, whereas the ten ISC dimensions in Martins and Da Veiga

(2014b) were changed to six dimensions' name after the factor and reliability analysis. These are the contributing factors that set off the inconsistency in the dimensions used to conceptualize ISC and also explain the nonexistence of common dimensions to model the ISC in the literature.

Based on analysis in Section 2.5.3 and its sub-sections, it could be concluded that ISC concept is relatively new and dimensions to represent the ISC are still evolving. There are various ISC concepts and models based on dimensions and the analysis found five main groups of ISC models in literature as discussed in in sub sections 2.5.3.1, 2.5.3.2, 2.5.3.3 and 2.5.3.4. The main different among this groups is the theories used to conceptualize the ISC. Next section discusses and concludes the relationships among all these ISC models. Two significant findings on ISC concept based on dimension are highlighted. First is the inconsistency of dimensions to represent ISC and second is Schein's OC as the most widely accepted in ISC conceptualization. The next sections conclude these two findings.

2.6.1 Inconsistency of Dimensions in ISC Concept

Previous section conludes that various sets of dimension have been used to conceptualize ISC in the literature. This means that there are many different ways were applied by researchers to define ISC. While this scenario provides more insights for researchers to study ISC effectively and meaningfully, this also indicates that ISC concept is still evolving and no mutual agreement is shown as to what is the most suitable concept should be adopted to be the underlying concept for ISC. This is consistent with Alnatheer (2015) who claimed that no agreement is achieved for factors required to create environment promoting the creation of security culture.

There are too many dimensions could be applied to model ISC. Although the review is based on studies published from the year of 2000 to 2017, the reality is that the additional articles only add to more versions of dimensions. These dimensions are different in terms of number and definition throughout the studies. To a certain extent, this analysis discovered different definitions were used for the same label of dimensions. The change of dimensions' definitions in several studies after factor and reliability analysis was also indicated. All of these findings suggest no common ISC concept in terms of dimensions used in the literature reviewed. Thus, the actual ISC

concept is still unclear (Tolah et al., 2017) and under study because the difference in dimensions is an indication that the understanding of security culture is still evolving (Kolkowska, 2011),

In a nutshell, there is no agreement on what are the most common or appropriate dimensions that could be used to conceptualize or model ISC. There is still no standard and clear dimensions that could be used to represent the ISC concept and applicable to all types of organization. This is actually a big gap in ISC literature since academicians and practitioners do not have a common or a standard reference model of ISC based on dimensions because of numerous dimensions to be considered. This lack of mutual agreement on what are the principles dimensions should be used in conceptualizing the ISC could confine the findings of ISC-related studies to be generalized and applied. For example, Tang et al. (2016) has found a causal relationship between OC and ISC particularly in terms of their dimensions. However, due to the inconsistency of ISC concept based on the dimensions in literature, these findings have some limitations since the authors themselves stated that there are might be some additional dimensions of ISC that could be considered.

In applying or generalizing the findings, one has to identify ISC concept used for particular study in order to ensure the ISC dimensions applicable for the findings. For example, the findings by D'Arcy and Greene (2014) that found security culture has significant impact on employees' ISP compliance intention could not be applied to all concept of ISC since this study used three dimensions, which are Top Management Commitment, Security Communications and Computer Monitoring. This is because another study by Alkalbani et al. (2015) also found that ISC has significant impact towards employee's compliance but used different dimensions to conceptualize ISC. These results show the differences of ISC dimensions but fail to prove how ISC influences employee's ISP compliance. This leads to lack of clear strategies of ISC that could be used by practitioners in establishing effective ISC in their organization.

The same scenario could happen to other ISC-related findings such as in the development of ISC application studies. Since ISC concept used is not standardized in covering basic ISC dimensions, the applications developed are limited on its applicability to represent holistic concept of ISC in the organization. All these scenarios indicate that all the studies could only claim from some ISC perspectives for their

findings but not from the holistic ISC concept. Although all the findings could complement each other in completing ISC dimensions, more comprehensive studies to produce a standard concept of ISC based on dimensions should be conducted so that the findings could be generalized and applicable to wider perspective of ISC.

2.6.2 Adopted Concepts in Modeling Information Security Culture (ISC)

The analysis reveals that most studies used literature review approach in conceptualizing the ISC. However, in terms of adopted concepts or theories, it was found that Organizational Culture (OC) are the most influential concept of ISC. This is consistent with conceptual and empirical findings that link ISC to OC such as in Tang et al. (2016). It also supports the argument in some studies such as those in Alnatheer and Nelson (2009); Reid et al., (2014); and Schlienger and Teufel (2003b) that ISC is a subculture of OC. From this perspective, although there are two main concepts of organizational culture, which are by Schein (1999) and Detert et al. (2000), the OC concept by Schein (1999) was found to be more widely used.

Figure 2.8 shows five main categories of ISC models based on adopted concepts. It shows most ISC models refer to Schein's OC. This is consistent with review by Pevchikh (2015) who discovered most of ISC concepts or models were influenced by Schein's OC in a way or another. Although there is another concept which is OB, the models based on this concept are recently influenced by Schein's OC. As discussed in Section 2.5.3.3, most OB based ISC models originate from series of studies on ISCA development. Recent development on ISCA and ISCF adopt Schein's OC and ISC by Van Niekerk and Von Solms (2006) in their models (Alhogail, 2015a; Alhogail, 2015b; Al Hogail & Mirza, 2015).

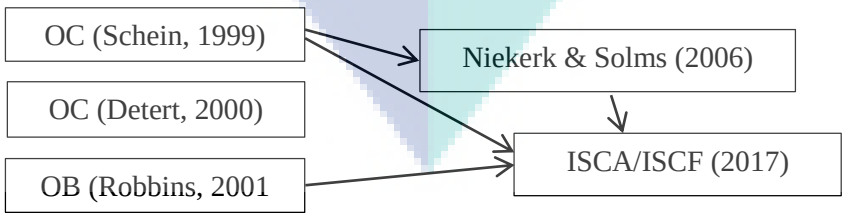


Figure 2.8 The Relationship among the Five Main Categories of ISC Models

Schein's OC concept was consistently used in this area since Schlienger and Teufel (2002, 2003a) until recent studies such as in Da Veiga and Martins (2015a); Martins and Da Veiga (2015b); and Chen et al. (2015). This is consistent with Kolkowska (2011) who argued this OC concept was successfully used to conceptualize ISC in many ISC-related studies. Furthermore, the level approach in Schein's model enables ISC conceptualization and assessment more transparent and comprehensive. For example, in Schlienger and Teufel (2003a), by using the OC model, the authors give the examples of security issues for each level contained in the model. In Okere et al. (2012), the authors revealed that using Schein's OC will make the assessment more comprehensive. Therefore, based on these facts, despite various concepts available in conceptualizing ISC, researchers could use Schein's OC for at least as a basic underlying concept to study ISC or any study that related to ISC.

As discusses in Section 2.5.3.2, ISC by Van Niekerk and Von Solms (2006) is one of the most common ISC model that adopted Schein's OC. Although ISCA/ISCF also adopted Schein's OC, it was found that ISCA/ISCF has inconsistency in its dimensions as discussed in Section 2.5.3.4 and Section 2.6.1. Furthermore, many recent studies of ISCA/ISCF also adopted Van Niekerk and Von Solms (2006) model to conceptualize ISC.

2.7 Organizational Behavior Concept

As discussed in previous section, despite the widely use of Schein' OC, Organizational Behavior (OB) concept by Robbins (2001) also contributes to the ISC model based on dimension in literature. Most of ISC models that use this concept is those researchers that develop and validate ISCA. The first ISC model based on this OB was developed by Martins and Eloff (2002). According to Martins and Eloff (2002), culture is how things are done in an organization and thus with the behavior of people. Therefore, Martins and Eloff (2002) believed that organizational behavior also has an impact on the information security culture of an organization.

As discussed in Section 2.5.3.3, this concept consists of three different levels, which are the individual, group and organizational levels as shown in Figure 2.9. These levels were adopted to be mapped into associated ISC dimensions as done by Martins and Eloff (2002). According to Martins and Eloff (2002), an organization that wants to

inculcate acceptable information security behavior in its employees needs to consider the impact of information security towards all the there levels in OB concept. For example, at individual level, each employee could be encouraged to report information security incident. At group level, management could be encouraged to support information security processes. At organizational level, an example could be the implementation of ISP. In summary, Martins and Eloff (2002) produced eight dimensions of ISC mapped from the three levels in OB as discussed in Section 2.5.3.3.

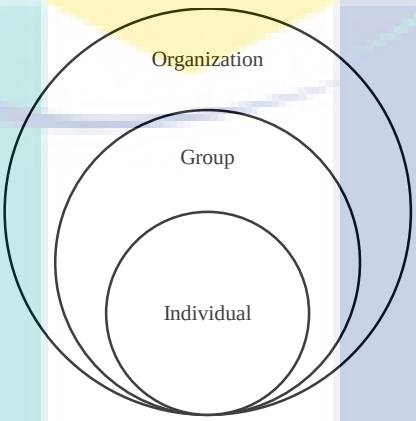


Figure 2.9 Organizational Behavior Concept

2.8 Schein's Organizational Culture Concept

In literature, the most adopted concept in understanding ISC is Organizational Culture (OC) by Schein (1999). According to Schein, OC could be explained by as consisting three levels, which are artifacts, espoused values and shared assumptions as shown in Figure 2.10.

According to Schein (1999), artifacts are what you can observe, see, hear, and feel, in an organization (Schein, 1999, p. 15). At this level, the culture is very clear and has an immediate emotional impact, which could be positive or negative, on the observer (Schein, 1999, p. 16). The second level is Espoused Value. According to Schein (1999), an organization's espoused values are the "reasons" an organizational insider would give for the observed artifacts. Espoused values generally consist of organization's official viewpoints, such as mission or vision-statements, strategy documents, and any other documents that describe the organization's values, principles, ethics, and visions (Schein, 1999, p. 17). However, it is possible for two organizations

to have very different observable artifacts and yet share very similar espoused values (Schein, 1999, pp. 18-19). The third level is Shared Tacit Assumptions. Often, these assumptions are formed in the organization's early years because certain strategies are proven to be successful (Schein, 1999, p. 19). The beliefs and values become tacit assumptions about nature of the world and how to succeed in it (Schein, 1999, p. 19).

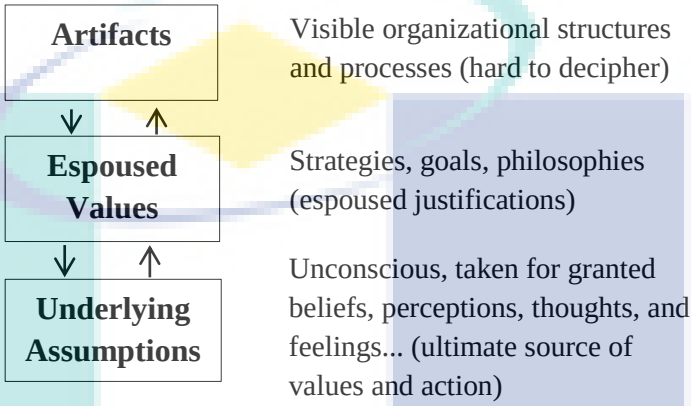


Figure 2.10 Organizational Culture Concept (Schein, 1999)
Source: Schein (1999)

2.9 The Use of Schein's Organizational Culture's Concept in Information Security Culture

As discussed in sub-section 2.5.3.1, most of the adopted concept used to conceptualized ISC is Organizational Culture (OC) concept by Schein (1999). This OC concept also widely accepted in ISC literature as most of the ISC concepts were influenced by this OC (Pevchick, 2015). Other recent studies that agree this OC is Flores and Ekstedt (2016) and Da Veiga and Martins (2017). However, these studies did not directly discuss ISC based on dimension and not included in this review. As discussed in previous section, Schein's OC concept is consisting three levels. These three levels of OC were adapted by Van Niekerk and Von Solms (2006) to conceptualize ISC; and they added one more level, which is Information Security Knowledge (ISK) as illustrated in Figure 2.11. They believed that this new level is important to differentiate OC from ISC. These three levels are for a normal OC; and ISK level underpins and supports all three "normal" levels of corporate culture to form an effective ISC in the organization. According to Van Niekerk and Von Solms (2006), if an organization attempts to foster a subculture of information security, all activities must be consistently performed within good information security practice. Therefore,

having adequate knowledge pertaining to information security is a prerequisite to perform any normal activity in a secure manner.

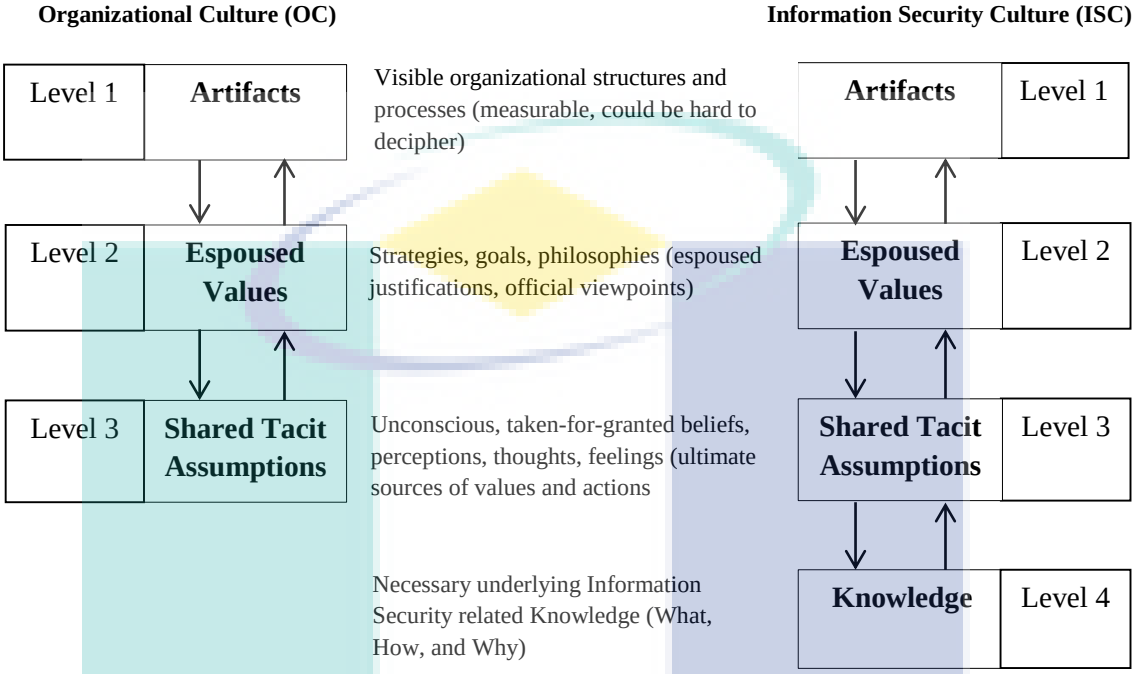


Figure 2.11 Adaptation of levels in Organizational Culture for ISC Framework
Source: Van Niekerk and Von Solms (2006)

The ISC framework by Van Niekerk and Von Solms (2006) focuses on functions and importance of information security knowledge towards three levels of OC in forming a stable ISC. According to Van Niekerk and Von Solms (2006), at the Artifacts level, the sufficient knowledge ensures the activities are performed in safely manner. At the Espoused Value level, the knowledge determines what to be included in a policy in order to adequately address the organization's information security needs. As for Shared Tacit Assumptions, this level consists of employees' beliefs and values. If such a belief should conflict with one of the espoused values, with adequate knowledge, knowing why a specific control is needed, might play a vital role in ensuring compliance (Schlienger & Teufel, 2003).

This ISC framework also suggests each of the underlying cultural level contributes towards the overall strength and stability of such a culture. Although this framework comprehensively explain the ISC concept based on levels, it does not clearly identified and defined specific factors or dimensions associated with each level.

Generally, some ISC factors were mentioned in explaining the model such as ISP. Nonetheless, no further clear identification of other factors or dimensions were suggested.

ISC concept defined with set of dimensions based on all ISC levels is crucial in conducting meaningful study to produce clear findings that could be applied to the study context. Furthermore, well-defined ISC dimensions assure the dimensions are accurately measured in producing more comprehensive assessments and understandable ISC concept. Okere, Van Niekerk, and Carroll (2012) claimed no current assessment is available to comprehensively assess all ISC levels. Moreover, Section 2.6.1 revealed that there is a lack of mutual agreement on the most comprehensive dimension to be used in conceptualizing ISC. Additionally, Section 2.6.2 concludes that the most accepted concept in conceptualizing ISC is Schein's OC; and ISC framework by Van Niekerk and Von Solms (2006) is the most consistent framework in adopting Schein's OC. Based on these arguments, a new set of dimensions to represent ISC concept based on levels in Schein's OC and ISC (Van Niekerk, 2006) was developed in this research.

2.10 Summary of Gaps in ISC Concept

Based on review and analysis in Section 2.8 until Section 2.9, the following are the gaps identified to be addressed in this research.

- There are inconsistency of dimensions in terms of name and definition used to conceptualized ISC and various theories and concepts have been adopted to study and model ISC.
- Most of the adopted concept used to model ISC is Organizational Culture (OC) by Schein (1999).
- ISC conceptual framework by Van Niekerk and Von Solms (2006) is one of the most referred concept and this concept consisting of four levels whereby three levels were adopted from Schein's OC. The forth level in this ISC concept is Information Security Knowledge.
- There is a lack of dimensions identified for each level in ISC conceptual framework by Van Niekerk and Von Solms (2006).

Based on these gaps, the objective is to formulate and validate the dimensions to represent ISC concept based on the levels of ISC (Van Niekerk & Von Solms, 2006) and OC (Schein, 1999) as mentioned in Research Objectives 1, 2 and 3 in Chapter 1.

2.11 Recent ISP Compliance/Incompliance Studies

Previous sections have reviewed and analyzed all related studies to identify the gaps and concepts in ISC models. It was found that there is a lack of agreement on the dimensions and approaches in conceptualizing ISC. However, the concept of OC by Schein and ISC conceptual framework by Van Niekerk and Von Solms (2006) are identified as the widely accepted concepts for ISC conceptualization. Since this research is to produce ISC model for ISP compliance behavior, this section focuses on another area of literature, which is ISP compliance behavior.

Considerable number of studies been conducted to investigate employees' compliance/incompliance behavior towards ISP (Sommestad, Karlzén, & Hallberg, 2017). These studies produced various models in predicting and explaining employees' behavior towards ISP in the organizations. These models adopted a considerable number of variables or factors drawn from various theories on human behavior that span from the disciplines of criminology, psychology, and sociology into the information systems field (Cram et al., 2017; Lebek, Uffen, et al., 2014; Sommestad, Hallberg, et al., 2014). Despite of many studies in this particular area, literature has shown the findings were scattered and mixed (Cram et al., 2017). There is still no clear winner on the most effective factors in predicting and explaining employees' ISP compliance behavior (Sommestad, Hallberg, et al., 2014). However, some common themes and significant findings were produced in this area.

In terms of behavioral factors, Sommestad, Hallberg, Lundholm, and Bengtsson (2014) uncovered more than 60 behavioral factors from various behavioral and psychological theories applied to study ISP compliance behavior. Although their systematic review revealed no clear winner among these factors and theories in explaining and predicting ISP compliance behavior, their meta-analysis found that there are some significant factors identified from Theory of Planned Behavior (TPB). The factors such as Attitude and Normative Belief were noticed to be among the most popular and the strongest predictors of ISP compliance behavior compared to others.

This is consistent with review conducted by Cram et al. (2017) and Lebek, Uffen, et al. (2014) that found Attitude, Normative Belief and Self-Efficacy are the strongest predictors of employees' ISP compliance behavior.

The reviews by Cram et al. (2017); Lebek, Uffen, et al. (2014) and Sommestad; Hallberg, et al. (2014) have produced important knowledge especially in providing clearer picture on behavioral factors in predicting the ISP compliance and incompliance behavior. However, in discussing studies of ISP compliance/incompliance behavior, besides behavioral factors, there are also other key elements such as behavioral theories, main dependent variables as well as non-behavioral factors used in the research models.

All three reviews focus on behavioral factors and does not provide intensive focus on main dependent variables. Although Lebek, Uffen, et al. (2014) was focusing on the theories used, however they did not focus specifically to ISP compliance behavior by considering all studies related to information security behavior. Moreover, their review was based on studies published from year 2000 until 2012. Therefore, while these reviews are important references for this thesis, new current review considering all aforementioned aspects should be conducted to get more comprehensive and latest knowledge. Table 2.3 shows key elements of reviews conducted in those three studies compared to current review from this research. Clearly, besides complementing the findings by providing more aspects than covered in previous reviews, this current review provides additional findings by selecting more recent studies. Although Cram et al. (2017) also reviewed the most recent studies, their review focus on behavioral factors of ISP compliance behavior only.

Table 2.4 presents selected studies of ISP compliance and incompliance studies based on theories and dependent variables published from 2010 – 2017. As many as 51 studies were selected after being filtered by certain criteria. Among the criteria are:

- The study must be about employees' security behavior towards ISP compliance/incompliance in the organizations.
- The study must have empirical findings in terms of relationships among constructs employed in the research model.
- The study must be published between 2010 - 2017.

Table 2.3 Comparison of Reviews

Criteria	Current Review	Sommestad, Hallberg, et al. (2014)	Lebek, Uffen, et al. (2014)	Cram et al. (2017)
Year of Studies published	2010 - 2017	1996 - 2012	2000 - 2012	2005 – 2016
Database/Resources used	ScienceDirect, IEEEXplore, SpringerLink, ACM, Wiley, Researchgate, InformsOnline, Emerald, AISeL, Google Scholar	Scopus, Inpec and Compendex, IEEE Xplore, Google Scholar	AISeL, ScienceDirect, IEEEXplore, JSTOR, SpringerLink, ACM, Wiley, Emerald, InformsOnline, Palgrave Macmillan	ABI/Inform, Business Source Complete, and Google Scholar
Scope of interest area of selected studies	ISP Compliance/Incompliance Studies	ISP Compliance/Incompliance Studies	Information systems (IS) security behavior	ISP Compliance
Specific objective of review	- To identify behavioral theories, non-behavioral theories and aspects as well as main dependent variables in recent ISP compliance literature - To identify the significant behavioral theories and factors in recent ISP compliance models	- To identify variables that influence compliance with information security - To identify the importance of these variables in ISP compliance /incompliance literature	- To provide an overview of theories used in the field of employees' information systems (IS) security behavior - To identify factors that proven to have significant influence on employees' security behavior	- To examine the strength of ISP compliance antecedents
Number of Studies Selected	51	29	114	25

It is worth to note that more than half of the studies selected in this recent review were not involved in both reviews from Sommestad, Hallberg, et al. (2014) and Lebek, Uffen, et al. (2014). The main reason is both studies review articles published until year 2012 only. The table presents three main categories, including main behavioral theory, other theory or aspects and main Dependent Variable (DV). Main behavioral theory column indicates recognized behavioral theories used in ISP compliance behavioral such as Theory of Planned Behavior (TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT) and Technology Acceptance Model (TAM). Other theories and aspects including motivation and learning theories as well as another aspect such as security training and awareness are indicated in the next column. Finally, main DV is presented in the last column.

Table 2.4 ISP Compliance/Violation Studies based on Theory and Dependent Variable Published for Period of 2010 – 2017

No.	Authors	Main Behavioral Theory used	Other Theory / Perspective / Aspect used	Main Dependent Variable used
1.	Bulgurcu et al. (2010a)	TPB, RCT	ISA, ISP Awareness, Outcome beliefs	Intention to Comply
2.	Siponen and Vance (2010)	Neutralization, GDT	NA	Intention to Violate
3.	Johnston and Warkentin (2010a)	PMT, Social Influence	NA	Intention to Comply
4.	Bulgurcu, Cavusoglu, and Benbasat (2010b)	NA	ISP Quality and Fairness	Intention to Comply
5.	Li, Zhang, and Sarathy (2010)	RCT, GDT	NA	Intention to Comply
6.	Johnston and Warkentin (2010b)	NA	Source Credibility Dimension	Intention to Comply
7.	Siponen, Pahnila and Mahmood (2010)	TRA, PMT, GDT,	Innovation Diffusion Theory	Actual Compliance
8.	Li, Sarathy and Zhang (2010)	GDT,	Organizational Justice	Intention to comply
9.	Son (2011)	GDT	NA	Actual Compliance
10.	Xue, Liang, and Wu (2011)	TAM	Justice Theory, Punishment	Intention to Comply
11.	Guo, Yuan, Archer, and Connelly (2011)	Composite Behavior Theory /Model (CBM), RCT, GDT	NA	Intention to Violate

Table 2.4 continued

No.	Authors	Main Behavioral Theory used	Other Theory / Perspective / Aspect used	Main Dependent Variable used
12.	Bulgurcu, Cavusoglu, and Benbasat (2011)	TPB	Organization-based Beliefs about the Consequences of Compliance and Non-Compliance	Attitude towards ISP Compliance
13.	Hu, Xu, Dinev, and Ling (2011)	RCT, GDT, Self-Control Theory, Moral Belief	NA	Intention to Violate
14.	Al-Omari, El-Gayar, and Deokar (2012)	TPB	ISA	Intention to Comply
15.	Hu et al. (2012)	TPB	Organizational Culture	Intention to Comply
16.	Vance, Siponen, and Pahnila (2012)	PMT, Habit	NA	Intention to Comply
17.	Hovav and D'Arcy (2012)	GDT	Security Countermeasures, National Culture, Social Status	Intention to Misuse
18.	Ifinedo (2012)	PMT, TPB	NA	Intention to Comply
19.	Vance (2012)	RCT, GDT	NA	Intention to Violate
20.	Guo and Yuan (2012)	GDT	NA	Intention to Violate
21.	Cox (2012)	TPB, PMT	Organizational narcissism	Actual Compliance
22.	Merhi and Midha (2012)	NA	Security Training	Intention to Comply
23.	Silvius and Dols (2012)	NA	NA – literature review on non-compliance factors	Non-compliance behavior
24.	Chen, Ramamurthy, and Wen (2013)	GDT	Compliance Theory Of Etzioni	Intention to Comply
25.	Borena and Bélanger (2013)	TPB	Religiosity	Intention to comply
26.	Barlow, Warkentin, Ormond, and Dennis (2013)	Neutralization	Framing Theory	Intention to violate
27.	Haeussinger and Kranz (2013)	NA	ISA and its antecedents	Intention to Comply
28.	Al-Omari, Deokar, El-Gayar, Walters, and Aleassa (2013)	TPB	Ethical Theory	Intention to Comply

Table 2.4 continued

No.	Authors	Main Behavioral Theory used	Other Theory / Perspective / Aspect used	Main Dependent Variable used
29.	Cheng, Li, Li, Holm, and Zhai (2013)	SBT, GDT	NA	Intention to Violate
30.	Humaidi and Balakrishnan (2013)	TPB, TAM	Security Training, Leadership Style	Actual Compliance
31.	Kajtazi and Bulgurcu (2013)	Escalation Of Commitment Theories, TPB	Agency Theory	Attitude towards ISP Compliance
32.	Kim, Yang, and Park (2014)	TPB, PMT, RCT, Neutralization	NA	Intention to Comply
33.	Aurigemma and Mattson (2014)	TPB, GDT	NA	Intention to comply
34.	Lebek, Guhr, and Breitner (2014)	NA	Transformational Leadership Style	Intention to Comply
35.	Kranz and Haeussinger (2014)	TPB	Organismic Integration Theory (OIT)	Intention to Comply
36.	Sommestad, Karlzén, and Hallberg (2014)	TPB, PMT and (anticipated regret)	NA	Intention to Comply
37.	Siponen, Adam Mahmood, and Pahnila (2014)	PMT, TRA	CET	Actual Compliance
38.	D'Arcy and Greene (2014)	NA	Security Culture and Employment	Intention to Comply
39.	Merhi (2014)	GDT	Task Dissonance	Intention to Comply
40.	Ifinedo (2014a)	TPB, SBT	SCT	Intention to Comply
41.	Alkalbani et al. (2015)	NA	Technology-Organization-Environment (TOE)	Actual Compliance
42.	Talib and Dhillon (2015)	NA	Intrinsic Motivation/Structured Empowerment Theory	Intention to comply
43.	Humaidi and Balakrishnan (2015)	HBM	Leadership Style	Actual Compliance
44.	Aurigemma and Mattson (2015)	TPB	NA	Intention to comply
45.	Ifinedo (2016)	GDT, RCT	Organizational Climate	Intention to comply
46.	Hovav and Putri, (2016)	PMT	Reactance Theory, Organizational Justice Theory	Intention to comply
47.	Yazdanmehr Wang (2016)	Norm activation Theory, Social Norms Theory	Ethical Climate Literature	Actual Compliance

Table 2.4 continued

No.	Authors	Main Behavioral Theory used	Other Theory / Perspective / Aspect used	Main Dependent Variable used
48.	Lee, Lee, and Kim (2016)	PMT	Prior security knowledge	Attitude towards ISP Compliance
49.	Bauer and Bernroider (2017)	TRA, Neutralization	ISA, KAB Model	Actual Compliance
50.	Bélanger et al. (2017)	TPB, PMT	Awareness of security policy change, organizational announcement	Actual Compliance
51.	Han et al. (2017)	RCT	Psychological Contracts Theory, Information Security Countermeasures	Intention to comply

*NA – the author (s) did not mention any theory/perspective for the factor applied in the study
Theories legend: TPB=Theory of Planned Behavior; RCT=Rational Choice Theory; PMT=Protection Motivation Theory; GDT=General Deterrence Theory; SCT=Social Cognitive Theory; TRA=Theory of Reasoned Action; TAM=Technology Acceptance Model; HBM=Health Belief Model; Composite Behavior Model (CBM); Knowledge, Attitude, and Behavior (KAB)

Table 2.4 reveals that main behavioral theories such as TPB, GDT and PMT are still dominating as found by Lebek, Uffen, et al. (2014). The table also indicates other aspects and theories such as Information Security Awareness (ISA), Leadership Style, ISP Awareness and Organizational Justice have gained more attention in recent ISP compliance/incompliance studies. The next sections discuss top behavioral theories in recent studies, which are TPB, GDT and PMT to analyze the role and significance of these theories in ISP compliance behavior literature.

2.11.1 Theory of Planned Behavior (TPB)

Theory of Planned Behavior (TPB) originates from Ajzen (1991) and it claims that human behaviors are essentially rational and largely rely individual's intention as illustrated in Figure 2.12. According to this theory, the prediction of intention relies on three-belief-based variables, which are Attitude towards behavior (ATT), Normative Beliefs (NB), and Perceived Behavioral Control (PBC). This theory has been proven to be a compelling social cognitive framework in explaining situation-specific influences on intentional behaviors across disciplines. Previous reviews by Lebek, Uffen, et al.

(2014) found that TPB is the most common behavioral theory applied in information security behavior literature for studies published between 2000 to 2012. Moreover, this theory is considered as one of the most well-established theories in the field of behavioral sciences, and the relationships described in the TPB are among the most frequently tested in ISP compliance and violation behavior models (Sommestad & Hallberg, 2013; Sommestad et al., 2017).

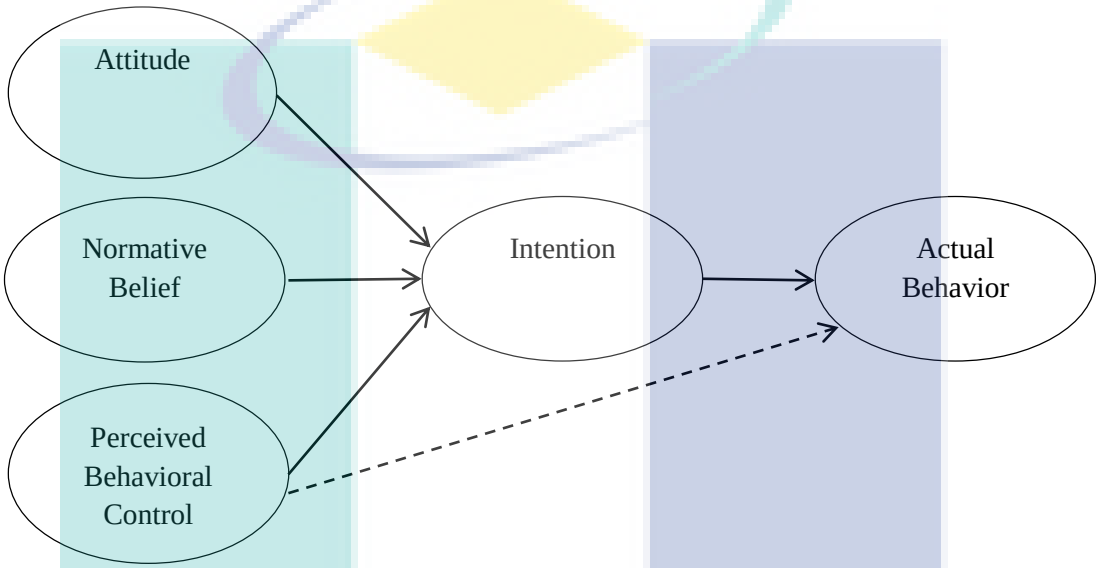


Figure 2.12 Theory of Planned Behavior (TPB)
Source: Ajzen (1991)

Apart from ATT and NB, most researchers applied Self-Efficacy (SE) rather than PBC in ISP compliance behavior literature. It is consistant with Fisfbein (2007), who argued that PBC essentially measures the same latent construct as SE and it originates from self-efficacy theory (Bandura 1977). Three behavioral factors of ATT, NB and SE have been widely utilized in ISP compliance behavior research (Lebek, Uffen, et al., 2014; Sommestad, Hallberg, et al., 2014; Sommestad et al., 2017). Table 2.4 shows that TPB has recently dominated the research models for explaining compliance behavior rather than violation behavior towards ISP. Table 2.4 also shows that all research models adopting this theory used main dependent variable of intention to comply (INT). In other words, the usage of this theory whether used as a single theoretical behavior (e.g. Cox, 2012; Hu et al., 2012) or a combination of other theories (e.g Bulgurcu et al., 2010b; Ifinedo, 2012), is always to investigate employees' ISP compliance behavior rather than ISP violation behavior in the organizations.

It is important to note that TPB is an extended version of another theory that has been used in ISP compliance behavior studies, which is Theory of Reasoned Action (TRA). Table 2.4 indicates TRA was recorded as many as three occurrences in recent studies. TRA is the work of Fishbein and Ajzen (1975) and has three similar phsycological constructs as TPB. However, this theory is not widely used lately due to its validity issue and limitation of applications (Kim et al., 2014). Siponen et al. (2014) applied this theory in a combination of multiple theories in their research model. It is worth to note that both TRA and TPB claimed that individual's actual compliance is influenced by his/her intention to comply towards the behavior. Another theory or model that has the same theme as TPB is Composite Behavior Model (CBM). It was proposed by Eagly and Chaiken (1993) and is an extension of TRA (Ajzen & Madden, 1986) and TPB (Ajzen, 1991). This model suggests that intention is the immediate cause of behavior and is influenced by attitude towards behavior, which in turn, is determined by the antecedents of habit, attitude toward target, utilitarian outcomes, normative outcomes and self-identity outcomes. Guo et al. (2011) employed these antecedents and constructs in CBM as the factors contributing to ISP violation intention in their study.

2.11.2 General Deterrence Theory (GDT)

According to D'Arcy and Herath (2011), General Deterrence Theory or GDT (Paternoster & Simpson, 1996) is one of the most widely applied theories in Information Systems (IS) security research, particularly within behavioral IS security studies. According to this theory, individuals are more likely to avoid deviant behavior when threat of sanctions or penalties increased. As shown in Figure 2.13, the pillars of this theory are sanction severity and detection probability.

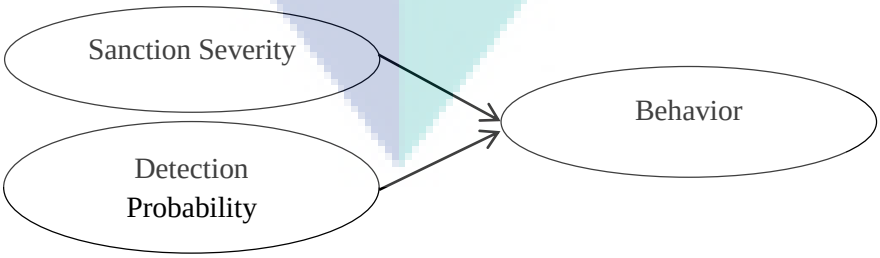


Figure 2.13 Two Pillars of General Deterence Theory

Consistent with review by Lebek, Uffen, et al. (2014) who found GDT is the second most used in information security behavior studies between 2000 – 2012, Table 2.4 shows that GDT also is mostly used in recent ISP compliance/incompliance studies, which placed it the second best after TPB. The main GDT factors employed in recent studies are perceived severity, perceived certainty, formal sanctions, informal sanctions and shame. However, it was found that most studies only used several factors from this theory and most of the time these factors were used as a representation or substitution of other factors from other behavioral theory such as in Chen et al. (2013), Cheng et al. (2013), Guo and Yuan (2012), and Li et al. (2010). For instance, the study of Cheng et al. (2013) used factors from SBT Theory to represent the factor of GDT informal control. This leads to the issue that the extensive use of this theory in ISP compliance/incompliance study failed to provide enough explanation and often have to be integrated and added to other factors from other behavioral theories. Additionally, the results and findings of the factors from this theory in regards to ISP compliance/incompliance, always have mixed findings (D'Arcy & Herath, 2011). This particular issue is discussed in Section 2.11.4.

Apart from that, the theory was either singly used (e.g. Guo & Yuan, 2012; Son, 2011) or combined with other theories (e.g. Chen et al., 2013; Hovav & D'Arcy, 2012; Hu et al., 2011; Li, Zhang, et al., 2010; Siponen & Vance, 2010; Vance, 2012). Unlike TPB, GDT was used not only in predicting and explaining ISP compliance behavior, it also applied in studies to understand and explain ISP violation behavior. This can be seen in Table 2.4, whereby half of research models applying this theory employed dependent variable of intention to violate rather than intention to comply or actual compliance. This is consistent as this criminology theory was originally developed to explain how to prevent people from engaging in deviant behaviors. It rests on the proposition that human behavior, to some degree, is rational; thus, can be influenced by incentives, particularly negative incentives inherent in formal sanctions (Wenzel, 2004).

It is worth to note that the root theory of GDT, namely Rational Choice Theory (RCT) (Becker, 1968; Paternoster & Simpson, 1996) also indicates high occurrences in recent ISP compliance/incompliance studies. It was found that both theories were always used together to form a theoretical foundation of research model in several ISP compliance studies (e.g Guo et al., 2011; Hu et al., 2011; Li, Zhang, et al., 2010; Vance,

2012). The reason is RCT and GDT are both related to each other. For instance, in contemporary Deterrence Theory (Pratt et al., 2010), several identical factors of RCT such as perceived risks and costs were included in both formal and informal sanctions of GDT. In addition, Table 2.4 also indicates that RCT was also commonly used in the study of ISP violation. Therefore, although recorded a high entry in terms of its popularity, both RCT and GDT in recent studies could be considered as dominant theories in the research models that aimed to explain the ISP violation behavior rather than compliance behavior. This fact also has been proved previously in review by D'Arcy and Herath (2011), suggesting that deterrence theory is a better predictor of negative behaviors such as abuse of IS resources as opposed to positive (compliant) behaviors.

2.11.3 Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) developed by Rogers (1983) was developed to help clarify fear appeals. It has been noted as one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions (Anderson and Agarwal, 2010). Figure 2.14 shows that, PMT consists of two main processes, which are threat appraisal and coping appraisal. The variables that capture threat appraisal are Perceived Severity and Perceived Vulnerabilty. As for coping appraisal, the variables that capture this appraisal are Response Efficacy, Response Cost and Self-Efficacy.

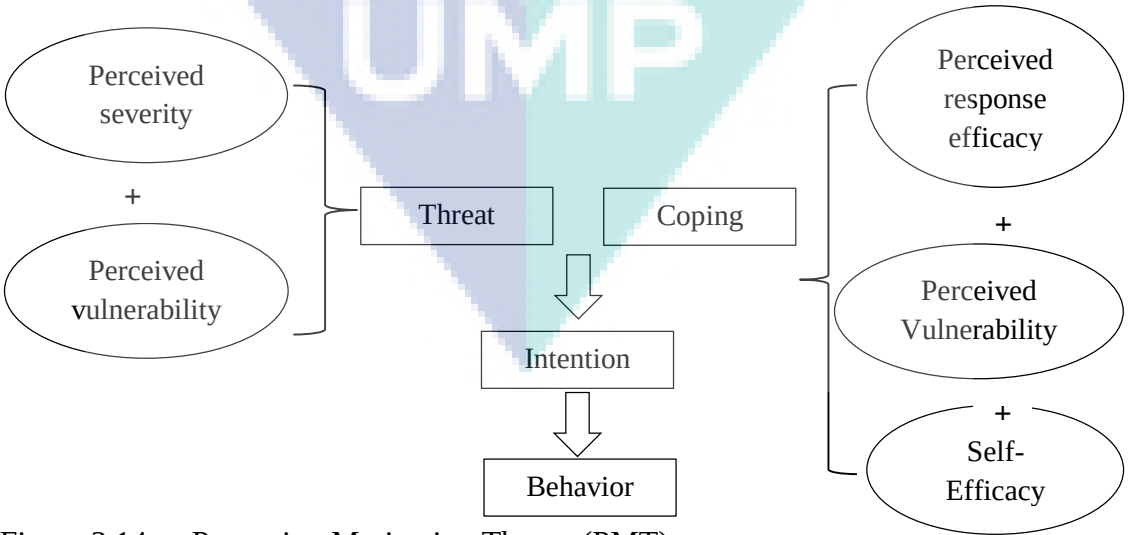


Figure 2.14 Protection Motivation Theory (PMT)

According to Pham, El-Den, and Richardson (2016), "PMT is a fear-based persuasive social communication tool which aims to influence cognition, attitudes, behavioral intentions and health behaviors (Maddux and Rogers, 1983; Rogers, 1975)". In ISP compliance research domain, PMT is considered as a competing theory to TPB (Sommestad, Karlzén, et al., 2014). Similar to TPB, the use of this theory in research models is always to study compliance instead of violation of ISP. As shown in Table 2.4, all eleven studies that employed this theory used intention to comply (INT) and actual compliance (ACT) as the dependent variables. Nevertheless, this theory is more appropriate to explain how security compliance is motivated by fear and threat as evident in Hovav and Putri (2016); Johnston and Warkentin (2010a); Lee et al. (2016); Siponen et al. (2014, 2010); Vance et al. (2012).

2.11.4 TPB as a Most Significant Theory in Recent ISP Compliance Behavior Study

Lebek, Uffen, et al. (2014) in their review has proven that TPB is among the most popular theories used in information security behavior research. They have shown that all the main constructs from this theory have more significant results compared to other constructs of other behavior theories such as PMT, TAM and GDT. The strength and significance of this theory and its main constructs in ISP compliance studies can also be seen in previous study conducted by Aurigemma and Panko (2011). They designed a composite framework of ISP compliance behavior using proven theories such as TPB, PMT, GDT and RCT with its respective constructs from previous studies. Specifically, after conducting extensive literature analysis to find significant theories and constructs, they selected TPB and its constructs as a core theoretical lense in their framework. The reason is they found that TPB was the most significant and dominant theories and all its constructs were often found significant in influencing employees' compliance behavior compared to others. Recent meta-analysis by Cram et al. (2017) also revealed that these three constructs have the strongest effect towards ISP compliance behavior with large magnitude of effect sizes for ATT as well as NB, and medium magnitude of effect size for SE.

Table 2.5 shows results of the relationships of these three constructs towards dependent variable used in studies published from year 2000 – 2017. Study by Humaidi and Balakrishnan (2013) was excluded because their study did not directly employ the

three constructs at all by representing them with other variables. In general, the table indicates that all these constructs were significant in influencing ISP compliance behavior of employees in the organizations. Specifically, according to Table 2.5, construct of ATT was 100% significant in all studies. In addition, due to the strength and acceptance of this construct in ISP compliance behavior study, some studies such as by Bulgurcu et al. (2011); Miranda Kajtazi and Bulgurcu (2013) have used this construct as dependent variable in their studies. In terms of NB and SE, although there are few studies found insignificant relationships, it is relatively small compared to other studies which found these constructs have strong and significant effect towards a DV. This scenario is consistent with prior review and meta-analysis conducted by Sommestad, Hallberg, et al. (2014), which found that all these three behavioral factors are significant in influencing employee's ISP compliance behavior. Thus, it is confirmed that all these TPB factors are the strongest and still relevant factors in ISP compliance behavior.

In comparison with two other competing theories, which are GDT and PMT, the findings show that main constructs of these two theories are not as convincing as TPB in predicting and explaining ISP compliance/incompliance behavior. Table 2.6 and Table 2.7 show the findings of relationships of main constructs of GDT and PMT towards particular Dependent Variables (DV) used in respective studies. As for GDT, the table clearly shows that its main constructs, namely Perceived Certainty of Sanctions (PCS), Perceived Severity of Sanctions (PSS) and Informal Sanctions (ISS) are not as strong as TPB's main constructs in terms of number of significant relationship towards DV. Most of GDT's main constructs could not provide a conclusive relationship towards DV and the findings are not consistent from one study to another. According to Table 2.6, unlike TPB, there is no 100% significant result of any of these main constructs towards DV. In fact, most of the time they produced mixed findings in these studies. For example, PCS was found significant in Li, Zhang, et al. (2010); and Siponen et al. (2010) but not significant in the studies of Cheng et al. (2013); Hu et al. (2011); and Son (2011). As for PSS, this construct was found significant in Aurigemma and Mattson (2014); Chen, Ramamurthy, and Wen (2013); and Cheng et al. (2013) but not in Hu et al. (2011); Li, Sarathy, et al. (2010); Son (2011). The same scenario also happened to construct of ISS, which was found

significant in Guo and Yuan (2012); and Siponen et al. (2010) but not in Li, Zhang, et al. (2010); and Siponen and Vance (2010).

Table 2.5 Results of TPB's Main Constructs in Recent ISP Compliance Behavior Studies

No.	Authors	Relationship towards Dependent Variable (DV) in a research model			DV Used
		ATT (β)	SE(β)	NB (β)	
1.	Hu et al. (2012b)	0.197***	0.360***	0.366***	INT
2.	Kim et al. (2014)	0.303***	0.07 NS	0.25***	INT
3.	Bulgurcu et al. (2010a)	0.25**	0.22**	0.29**	INT
4.	Kranz and Haeussinger (2014)	0.242***	0.084*	0.216***	INT
5.	Al-Omari et al., (2013)	0.12***	0.25***	0.14***	INT
6.	Sommestad, Karlzén, et al. (2014)	0.35**	0.21**	0.22**	INT
7.	Ifinedo (2014a)	0.63***	0.18*	0.15*	INT
8.	Ifinedo (2012)	0.48***	0.17**	0.19**	INT
9.	Cox (2012)	0.12*	0.15*	0.73*	INT
10.	Bulgurcu et al. (2011)	As dependent variable	NA	NA	ATT
11.	Aurigemma and Mattson (2014)	0.584***	NA	NA	INT
12.	Borena and Bélanger (2013)	0.447***	0.316***	0.352*** (ATT) NS (INT)	INT
13.	Al-Omari et al. (2012)	0.206***	0.119***	0.233***	INT
14.	Kajtazi and Bulgurcu (2013)	As dependent variable	NA	NA	NA
15.	Aurigemma & Mattson (2015)	NA	0.390***	NA	INT
16.	Bélanger et al. (2017)	0.364***	0.036 NS	-0.052 NS	INT

*p < 0.05, ** p < 0.01, *** p < 0. 001
ATT - Attitude
NB – Normative Belief
SE – Self-Efficacy
INT – Intention to Comply
ACT – Actual Compliance
NS – Not Significant
NA – Not used in the study

In addition, some studies did not apply all of these main constructs in the models as labelled NA in Table 2.6. As discussed earlier in Section 2.11.2, most studies adopting GDT did not employ all the main constructs of this theory. To a certain extent,

there is no clear indication of what are the main constructs of this theory. At some point, it looks like three constructs selected in Table 2.6 are the main constructs but some studies did not use these main constructs at all. For example, study in Guo et al. (2011) employed Workgroup Norm to represent ISS and Perceived Sanctions for PCS and PSS. On the other hand, some studies combined these particular constructs in the research model.

Unlike TPB, GDT constructs were not consistently used in most ISP compliance behavior models. In fact, there is no consistency in terms of usage of GDT's main constructs from one study to another. As can be observed in Table 2.6, most studies applied PCS and PSS constructs as Independent Variables (IV) but other studies combined these two constructs to represent IV of Formal Sanctions in their research models such as in Guo, Yuan, Archer, and Connelly (2011); Siponen and Vance (2010); and Vance (2012). Moreover, some studies used one of these two constructs (Chen et al., 2013) and interestingly some studies did not use these two constructs (e.g Guo & Yuan, 2012) at all even though they are the most common constructs for this theory. All these arguments have led to a conclusion that main constructs of this theory were not convincing enough to explain ISP compliance/incompliance behavior of employees in the organization.

As for main constructs of PMT, although Table 2.7 shows stronger results compared to GDT in terms of significant relationship, it still has some issues especially in terms of usage and applicability of its main constructs in research model. Table 2.7 shows many cases of NA (Not Applicable) of constructs of this theory in a research model. This means that most studies using PMT have not applied all the main constructs in the research models. Only Ifinedo (2012); Vance, Siponen, and Pahnila (2012) applied all PMT main constructs as a single factor (without combination) towards a DV in their models. Some studies have combined certain constructs and this somehow suggests that a single construct of PMT is not strong enough in providing a significant relationship towards a DV. It is consistent with Sommestad, Karlzén, et al. (2014) that proved additional PMT constructs into TPB framework did not provide much different in explaining ISP compliance behavior.

Table 2.6 Results of GDT's Main Constructs in Recent ISP Compliance Behavior Studies

No.	Study	Relationship towards dependent variable in a research model			DV Used
		PCS (β)	PSS (β)	ISS (β)	
1.	Hu et al. (2011)	-0.082 NS	-0.087 NS	NA	ITV
2.	Son, Jai-Yeol (2011)	0.05 NS	0.06 NS	NA	ACT
3.	Li, Zhang, et al. (2010)	0.24**	-0.12 NS	- 0.09 NS	INT
4.	Cheng et al. (2013)	0.27 NS	-0.311****	NA	ITV
5.	Hovav and D'Arcy, (2012)	-0.20** for Korean Sample, -0.06 NS for US Sample	-0.14** for US Sample, 0.04 NS for Korean Sample	NA	ITV
6.	Siponen et al. (2010)	0.09* (combined)			ACT
7.	Siponen and Vance (2010)	0.4 NS (combined)		-0.07 NS	ITV
8.	Guo and Yuan (2012)	NA	NA	-0.41****	ITV
9.	Aurigemma and Mattson (2014)	NS	0.282*	NA	INT
10.	Chen et al. (2013)	NA	Significant^	NA	INT
11.	Vance (2012)	-0.02 NS (combined)		-0.10*	ITV
12.	Guo et al. (2011)	-0.053 NS (combined)		0.225****	ITV
13.	Li, Sarathy, et al. (2010)	0.13**	0.06 NS	NA	INT
14.	Merhi (2014)	Significant^	Significant^	NA	INT
15.	Ifinedo (2016)	0.02 NS	0.37***	NA	INT

*p < 0.1 **p < 0.05, *** p < 0.01, **** p < 0. 001
^using ANOVA analysis
PCS - Perceived Certainty of Sanctions
PSS - Perceived Severity of Sanctions
ISS - Informal Sanctions
INT – Intention to Comply
ACT – Actual Compliance
ITV – Intention to Violate
NS – Not Significant
NA – Not used in the study
DV – Dependent Variable
(combined) – the result is a combination of effect of particular constructs towards dependent variable

Table 2.7 Results of PMT's Main Constructs in Recent ISP Compliance Behavior Studies

No.	Study	Relationship towards dependent variable in a research model					DV
		PV (β)	PS (β)	RE (β)	SE (β)	RC (β)	
1.	Siponen et al. (2014)	0.062**	0.069**	0.13 NS	0.087***	NA	ACT
2.	Ifinedo (2012)	0.20***	-0.20**	0.27***	0.17***	-0.12 NS	INT
3.	Sommestad et al. (2014)	0.04 significant* (combined)		0.01 NS (combined)			INT
4.	Vance et al. (2012)	0.10 NS	0.27***	-0.21***	0.34***	-0.18**	INT
5.	Johnston and Warkentin (2010a)	NA	NA	0.213***	0.187***	NA	INT
6.	Cox (2012)	0.9**	0.39 NS	NA	NA	NA	ATT
7.	Siponen et al. (2010)	0.12** (combined)		-0.02 NS	0.17**	NA	ACT
8.	Kim et al., (2014)	NA	NA	0.266****	NA	NA	INT
9.	Hovav & Putri (2016)	0.168* (combined)		0.330***	0.091 NS	NA	INT
10.	Lee et al. (2016)	0.48****	NA	NA	NA	NA	ATT
11.	Bélanger et al. (2017)	0.434****	0.135**	NA	NA	NA	ACT

*P < 0.1, **p < 0.05, ***p < 0.01, **** p < 0. 001
NS – Not Significant
NA – Not used in the study
PV - Perceived Vulnerability
PS - Perceived Severity
RE - Respond Efficacy
SE - Self-Efficacy
RC - Respond Cost
DV – Dependent Variable
(combined) – the result is a combination of effect of particular constructs

2.11.5 Dependent Variables in ISP Compliance/Incompliance Studies

In studying and investigating ISP compliance/incompliance behavior of employees in the organization, there were two types of categories of Dependent Variables (DV) used by the researchers. In the recent literature of ISP compliance behavior field, the first category is the studies that used ISP compliance behavior as the DV. It generally refers to employee behavior that is compliant with organizational

security policies (Bulgurcu et al., 2010a; Chan, Woon & Kankanhalli, 2005; Herath & Rao, 2009a, 2009b; Son, 2011). There are two types of variable recently used for this category, which are Intention to Comply (INT) and Actual Compliance (ACT). Figure 2.15 shows percentage of DVs used in recent literature between year 2010 until 2017 extracted from Table 2.4. It shows that more than 50% of the studies used INT as DV in investigating employees' ISP compliance behavior compared to ACT with only 19%. Previous reviews by Sommestad, Hallberg, et al. (2014) and Lebek, Uffen, et al. (2014) also found that most studies used intention instead of actual compliance.

One of the factors contributing to this matter is that most recent studies employed TPB in their research models. In ISP compliance research domain, this theory concerns with intention to comply as a result of other factors (attitude, normative belief and self-efficacy) of this theory (Sommestad & Hallberg, 2013). Another explanation for many studies employing intention to comply is due to the fact that actual compliance behaviors are not readily observable or objectively measurable as they are "ideographic in nature" (Workman et al., 2008). Previous studies on behavioral theories mostly assessed behavioral intentions rather than actual behavior due to the difficulties in observing employees' actual security behavior, especially in organizational settings (Hu et al., 2012; Sommestad et al., 2017; Vroom & Von Solms, 2004). Moreover, Fishbein and Ajzen (1975) stated that intentions are proximal cognitive antecedents of actions or behavior. In addition, the influence of intention on behavior has been rigorously tested and is well established in the literature of ISP compliance research. According to Guo et al. (2011), replicating the link from intention to actual behavior in the proposed model may not add much theoretical contribution.

The second main category of DV used in this research stream is the variable to investigate employees' behavior towards violation of ISP. ISP abuse refers to any act by employees using computers against the established rules and policies of an organization for personal gains (Hu et al., 2011). Only eight studies employed this DV and most of them applied factors and theories of GDT, RCT and Neutralization. Direct justification to this scenario is that these criminology theories are suitable for understanding and explaining violation behavior. Therefore, most studies employing these theories used intention to ISP violation rather that compliance.

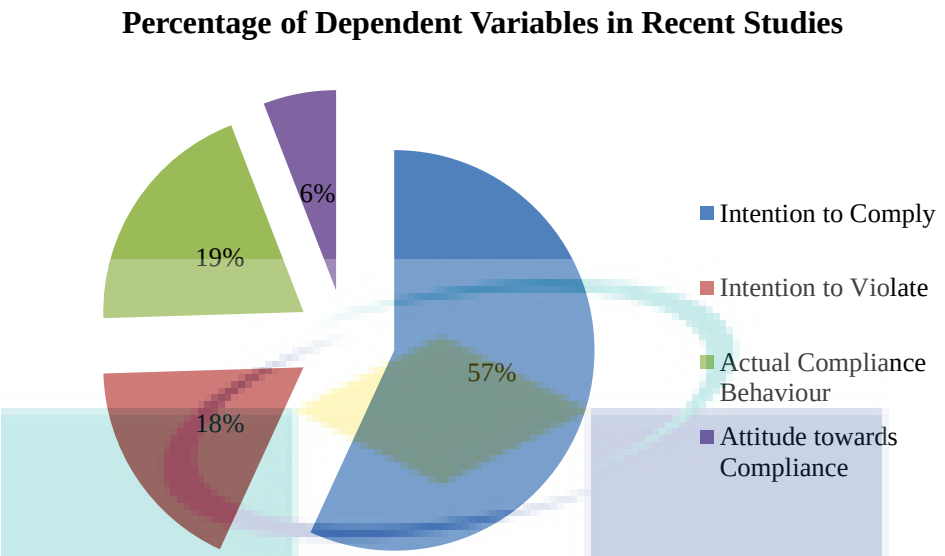


Figure 2.15 Percentage Dependent Variables Used in Recent Studies (2010 – 2017)

2.11.6 Intention to Comply and Actual Compliance in TPB

As mentioned in previous section, most studies of ISP compliance used dependent variable of intention to comply (INT) instead of actual compliance behavior (ACT). This scenario can be justified due to certain difficulties with observing actual security-compliant behavior (Sommestad et al., 2017; Vroom & Von Solms, 2004). For instance, ISPs comprise of several guidelines, which some are not practical to be measured and their standards as well as the penalties imposed in non-compliance situations can greatly vary within and between organizations (Ratnamalala & Marett, 2014).

While several researchers demonstrated a strong and consistent relationship between the two constructs of INT and ACT (Venkatesh, Morris, Davis, & Davis, 2003; Webb & Sheeran, 2006) in non-information security context, measurement of ACT is argued to be difficult due to the sensitive context of information security (Anderson & Agarwal, 2010; Vroom & Von Solms, 2004), the large and diverse sample sizes (Bulgurcu, Cavusoglu, & Benbasat, 2009a, 2009b; Bulgurcu et al., 2010a) and theoretical background of the applied theory (Siponen & Vance, 2010). In addition, some authors (Anderson & Agarwal, 2010; Siponen & Vance, 2010) argued the relationship between INT and ACT is grounded in TPB and TRA by Abraham (2011) and has been shown to be proven empirically by Anderson and Agarwal (2010). In fact,

INT has been demonstrated as a good predictor of actual behavior (Lebek, Uffen, et al., 2014) and it has been used widely in this research area recently as depicted in Figure 2.15.

From TPB perspective, given some actual control over the behavior in question, people are expected to follow their intentions upon confronting appropriate impetus. Thus, behavioral intention is assumed to be the immediate antecedent of actual behavior (Ajzen, 2002). A number of studies emphasized the relationship between employees' INT and ACT (Limayem & Hirt, 2003; Siponen, Pahnila, & Mahmood, 2007; M. Siponen et al., 2010). Therefore, due to all these arguments, the use of INT is more significant and practical than ACT when utilizing TPB in a research model.

2.11.7 Control Variables in ISP Compliance Behavior Studies

According to Chen et al. (2013), "previous research in the IS security literature, for instance, suggests that individual characteristics such as age and gender are related to security policy compliance intention (Leonard & Cronan, 2011.; Straub & Welke, 1998)". However, in recent ISP compliance behavior studies especially those using ISP Compliance Intention (INT) as main dependent variable (DV), there are mixed approaches and findings pertaining to the control variable (CV). In general, mixed findings in terms of inclusion of CV in ISP compliance behavior studies were discovered, particularly in the studies using TPB in the research models. Specifically, most authors did not include any control variables in the research models (e.g. Kim et al. (2014); Aurigemma & Mattson (2015); Aurigemma & Mattson (2014); Sommestad, Karlzén, et al. (2014); Borena & Bélanger (2013); Al-Omari et al. (2013); Al-Omari et al. (2012); Ifinedo (2012)).

On the other hand, some studies included CVs with mixed findings in terms of their relationships with INT. Among common CVs used are age, gender, working experience and education. However, there is no strong evidence that these particular CVs affect INT construct. Whilst, some studies found these CVs have significant effects on INT; most studies found that these CVs also are not significant in influencing INT. For examples, Kranz & Haeussinger (2014) found that CVs of age and gender did not have significant influence towards INT; whereas Ifinedo (2014a) found that age has significant influence towards INT.

There is no solid justification stated by the authors regarding the use of CVs in their studies. For examples, the inclusion of CVs in Hu et al. (2012) is based on suggestion from previous studies whereas for Bulgurcu et al. (2010a), the inclusion is to examine for the impacts of CVs on an employee's intention to comply. As in Ifinedo (2014a), the inclusion of CVs is "to enhance the insight into ISSP compliance". Some studies such as Kranz & Haeussinger (2014) did not state any justification for CVs inclusion. These scenarios suggest that the decision to include CVs to examine their effect on INT is still not clear and mostly depends on the authors' decision. However, according to Becker (2005); Bernerth & Aguinis (2016); Breaugh (2006), the decision to include CV in a study should be supported by theory. Therefore, careful attention should be given to this issue and strong justification must be provided in order to include CVs in this particular area of study.

Nevertheless, there are some interesting findings that is worth to note. Since effects of industry type and occupation in all recent studies were found as to have no significant influence on INT (Bulgurcu et al., 2010a; D'Arcy & Greene, 2014; Haeussinger & Kranz, 2013; Ifinedo, 2014a; Kranz & Haeussinger, 2014), this suggests that employees' ISP compliance intention is not affected by organization type. In other words, there is no difference in employees' intention to comply with ISP even though they come from different type of organization such as Government, Healthcare, Retail/wholesale, Consulting, Financial Services, IT and Telecom, Manufacturing, Education and others.

2.11.8 Conclusion on Theories in ISP Compliance Studies

Table 2.8 depicts a summary of comparisons among these leading theories in recent studies. The comparison criteria are based on the objective to find the most significant theory in recent ISP compliance behavior studies published between the year 2000 to 2017. Since ISC is synonym with promoting desired compliance behavior (Alfawaz et al., 2010; Vroom and Von Solms, 2004), it is important to compare these theories in terms of number of occurrences in ISP compliance behavior models rather than violation behavior models. Moreover, due to significance usage of intention to comply (INT) in ISP compliance studies, comparisons among these three theories from this aspect also illustrated in the table. Consistent with previous review by Lebek, Uffen, et al. (2014), the table shows that main constructs of TPB are the most

significant predictors of INT compared to other main constructs from competing theories of GDT and PMT. It is worth to note that since these findings are based on articles published from 2010 to 2017, the results might change with additional articles. However, considering the facts from Table 2.8 that main constructs of TPB were consistently found significant towards INT, additional articles woúld not change the fact that TPB is the most significant theory used to explain ISP compliance behavior.

Furthermore, due to GDT's originality in explaining violation behavior, it is more appropriate to be applied in ISP incompliance behavior studies. Although some indicators suggest PMT is also a significant theory in this area of study, most of the time the use of this theory does not consider a whole set of factors from this theory. Moreover, PMT is fear-based theory and used to explain how security compliance is motivated by fear (Pham et al., 2016). It is indeed contradicted with this research objective, which is to study compliance based on ISC, of which is not a fear-based concept. Interestingly, one of the most significant factors from this theory, which is self-efficacy, is similar with self-efficacy in TPB. All in all, besides it is the most appropriate theory in studying motivational perspective of ISC, TPB is also the most significant theory used in ISP compliance behavior and its main constructs are the strongest predictors for INT.

Table 2.8 Summary of Comparisons among TPB, GDT and PMT

Theory	**Main Constructs**	**No. of occurrences as IV without combination with other IV in ISP Compliance Behavior Model**	**No. of occurrences as IV in relationship with INT**	**No. of significance relationship with INT**
TPB	ATT	13	13	13
	SE	13	13	11
	NB	12	12	10
GDT	PCS	6	5	3
	PSS	7	6	4
	ISS	5	1	0
PMT	PV	6	2	1
	PS	5	2	2
	RE	7	5	5
	SE	6	4	3
	RC	2	2	1

2.12 ISC as a Multidimensional Concept

In literature, generally there are two types of ISC construct to conceptualize ISC. The first one is unidimensional construct. It is a form of general aspect of ISC construct measured by several reflective indicators. Example of studies that applied this type of construct are as in Alharbi (2017); Flores and Ekstedt (2016); Knapp, Marshall, Rainer, and Ford (2006). The second conceptualization is ISC as multidimensional construct forming by lower order latent constructs as used in D'Arcy and Greene (2009, 2014). This type of construct is also called multidimensional second-order construct. The concept operationalize in this way is called multidimensional concept.

From the perspective of this thesis, the second approach of conceptualization provides more comprehensive findings by providing clearer aspects of an ISC concept. Since these dimensions represents distinct aspects of ISC used in the study, they also represent the guidelines in terms of aspects to be used in establishing ISC. For example in D'Arcy and Greene (2014), the authors used dimensions of Top Management Commitment, Security Communications and Monitoring in representing ISC concept. They found out that these dimensions were significant in forming ISC concept and could be used as a guideline to establish ISC in an organization.

On the other hand, the studies which did not employ particular dimensions to represent their ISC concept could not provide clear and distinct aspects of ISC to be used in assessing and cultivating ISC. Instead of using particular dimensions, the ISC concept in these studies are conceptualized and operationalized as reflective constructs measured by several interchangeably indicators that usually representing the same aspect of ISC. Therefore, these studies could only provide findings on the relationship between ISC and security behavior and could not provide clear elements of ISC under study.

2.13 The Influence of ISC towards Employee's Security Behavior

Reviews on both ISC and ISP compliance behavior literature in previous sections revealed the significant concepts and theories that could be used as theoretical background in developing ISC model for ISP compliance behavior. The key finding in ISC literature review is the issue of ISC conceptualization based on dimensions, whereas the key finding in ISP compliance behavior literature review is that TPB is

found to be the most significant theory for predicting and explaining the behavior. Therefore, this section reviews current findings on the relationship between ISC and employees' security behavior from the combination of two perspectives; ISC concept and TPB.

In order to investigate current findings in more detail, a systematic review was conducted. Based on the same 239 articles found in Section 2.5, the search is narrowed-down to select only ISC articles that have examined relationship with security behavior and other additional inclusion criteria. This was carried out by evaluating the title, abstract, and full-text of the studies. In summary, the inclusion criteria are as in the following:

1. The article must report empirical findings on relationship between ISC and employee's security behavior in organizational settings
2. ISC concept used in the study must be clearly conceptualized and operationalized
3. ISC construct is used as predictor or antecedent for security behavior constructs in the research model

2.13.1 Empirical Findings on the Effect of ISC towards Information Security Behavior

After applying selection criteria outlined in previous section, five studies selected for further analysis. One study by Dugo (2007) that found from the references of the selected papers also included and the final total number of selected papers is six. This is an indication that instead of widely recommendation of ISC establishment in guiding employees' security behavior, there is actually lack of findings to support the relationship. Table 2.9 shows statistical findings on the relationships between ISC and particular constructs of security behavior in terms of path coefficient (β) and correlation coefficient (r) for the selected studies. Security behavior constructs consist of Attitude (ATT) and Normative Belief (NB) as well as the main Dependent Variable (DV) of interest in the selected studies. The table also shows ISC concept based on type of construct with particular constructs that used as dimensions. Interestingly, since the behavior constructs of ATT and NB in the table are among the main constructs of TPB, this suggests that TPB is the most appropriate theory in studying the relationship between ISC and employee's security behavior.

Table 2.9 indicates mixed findings from these six studies. Specifically, Dugo (2007) discovered no significant relationship was found between ISC and ATT as well as between ISC and NB in line with ISP violation. This finding was also reported by Sommestad, Hallberg, et al. (2014) in their systematic literature review suggesting that security culture is a weak predictor towards DVs used in security behavior literature. Dugo (2007) concluded that although an organization has strong ISC, it could not influence the employees to weaken their attitude and normative belief towards ISP violation. The reason is ISC concept used in his study is considered as a longer-term organizational issue which commonly attributed to organizational culture. Consequently, according to the author, it has weaker influence compared to shorter-term organizational issues such as recent observations or experiences concerning information security in the workplace, which may have stronger influence on employees' attitude and subjective norm towards ISP intentional violation.

Table 2.9 Findings of Relationships between ISC and Security Behavior Constructs

		Path Coefficient, β or Spearman Correlation, r between ISC and Particular Security Behavioral Constructs		
Study	**ISC Concept (Dimension)**	**Main Dependent Variable**	**ATT**	**NB**
Dugo (2007)	Unidimensional Construct	NA	β=0.019 NS	β=-0.015 NS
D'Arcy & Gwen Greene (2009)	Higher-order Multidimensional (TMC, COM)	β=0.552****	NA	NA
D'Arcy & Greene (2014)	Higher-order Multidimensional (TMC, COM, MON)	β=0.636***	NA	NA
Alkalbani et al. (2015)	Represented by TMC ACC ISA	β=0.18*** (TMC) β=0.24*** (ACC) β=0.18*** (ISA)	NA	NA
Parsons et al. (2015)	Unidimensional Construct	NA	r=0.703	NA
Flores & Ekstedt (2016)	Unidimensional Construct	NA	β=0.24***	β=0.46***

*p <0.1, **p < 0.05 ***p < 0.01 ****p < 0.001
TMC – Top Management Commitment
COM – Security Communications
MON – Security Monitoring
NA – Not Applicable/not examine the relationship
NS - Not Significant

On the other hand, study by Parsons et al. (2015) unveils that organizational ISC has significant influence on employees' attitude towards policy and procedures. Unlike findings by Dugo (2007), Parsons et al. (2015) claimed that an organization that has better ISC is more likely to have better employees' attitude towards ISP. Obviously, these mixed findings could be justified by two different aspects applied in these two studies. First, whilst Parsons et al. (2015) used attitude towards following ISP as the main DV; Dugo (2007) employed attitude towards ISP violation as his main DV of interest. In security behavior literature, these variables of compliance and violation are opposite to each other and there are also differences in terms of theories and approaches used for these two DVs as discussed in Section 2.11.5.

Second, besides using different main DV, these two studies employed different ISC constructs in terms of conceptualization and operationalization. As depicted in Table 2.2 in Section 2.5, ISC concept in Parsons et al. (2015) was conceptualized by conducting literature review focusing on organizational culture by Schein (1992), organizational climate, rewards and punishment. In contrast, study by Dugo (2007) has used conceptualization and operationalization of ISC that originate from Knapp et al. (2006). As shown in Table 2.2, the ISC model by Knapp et al. (2006) was originally developed from a mixed-mode (qualitative and quantitative) study of developing and testing a theoretical model to demonstrate the influence of top management support on ISC and level of security policy enforcement. Therefore, by using different approaches and perspectives, the ISC concepts produced are also different. Moreover, in terms of operationalization, both studies used different items to measure ISC construct. All these differences have produced different ISC concepts, which in turn have influenced the results and findings in both studies.

In security behavior literature especially in ISP compliance behavior, it is widely accepted that three main constructs of Theory of Planned Behavior (TPB), which are ATT, NB and SE are the most common and significant behavioral factors. Interestingly, apart from Dugo (2007) and Parsons et al. (2015), studies that comprehensively examine the relationship between ISC and ISP compliance behavior involving these three contructs are still lacking. As shown in Table 2.9, besides studies by Dugo (2007); Parsons et al. (2015); Flores and Ekstedt (2016), other studies did not examine these

relationships as indicated by NA (Not Applicable) tag in the table. As a matter of fact, no study examines the relationship between ISC and SE.

In fact, most studies investigated the direct effect of ISC towards main DV such as by Alkalbani et al. (2015); D'Arcy and Greene (2014); and D'Arcy and Greene (2009) as shown in Table 2.9. While these studies have given useful findings to practitioners and academia, the impact of ISC towards these particular relationships should be investigated because these behavioral factors are proven to be the most significant factors of employees' security behavioral intention (Lebek, Uffen, et al., 2014). Furthermore, according to TPB, individual intention towards particular behavior depends on his/her attitude, normative belief and self-efficacy. Therefore, the findings on these particular relationships will provide more comprehensive knowledge and understanding on ISC effects towards security behavior. As a result, it provides more convincing findings in explaining the actual influence of ISC towards security behavior.

Study by Flores and Ekstedt (2016) is the only recent study that examined more comprehensive relationships between ISC and security behavior by providing more comprehensive findings of relationship between ISC and employees security behavior compared to other studies. In particular, they found ISC has significant effect on Attitude and Normative Belief towards resisting social engineering. This knowledge is crucial in providing a comprehensive understanding on the influence of ISC towards security behavior especially from TPB context. Since security behavioral intention depends on these three main TPB constructs of Attitude, Normative Belief and Self-Efficacy, the findings provide additional knowledge on how significant ISC influence on these behavioral factors, which in turn will influence their security behavioral intention. Additionally, Flores and Ekstedt (2016) also examined mediation effect of three behavioral factors on the relationship between ISC and employees' security behavioral intention. These examination and findings are also important as they indicated the roles of three behavioral factors in influencing the relationship between ISC and employee's security behavioral intention.

However, from the perspective of this review, instead of providing more comprehensive findings on the relationship between ISC and employees' security behavior, several limitations were noted in the findings by Flores and Ekstedt (2016) to conclusively support the relationship between ISC and employee's security behavior.

First, the main DV used is quite different from those commonly used in security behavior especially in ISP compliance behavior. In ISP compliance behavior literature, common main DVs are Intention to Comply, Attitude towards ISP Compliance, Actual ISP Compliance and Intention to ISP Violation (Lebek, Uffen, et al., 2014; Sommestad, Hallberg, et al., 2014). Second, one TPB behavioral factor is still not examined in the study, which is Self-Efficacy. Since TPB suggests behavioral intention is determined by Attitude, Normative Belief and Self-Efficacy, these whole set of behavioral factors need to be examined to profound knowledge on the relationship between ISC and employee's security behavior. Last but not least, the study by Flores and Ekstedt (2016) also did not apply ISC as the sole predictor for security behavior. Specifically, instead of ISC, they also examined the effect of Information Security Awareness and Transformational Leadership towards employees' security behavior. Therefore, their findings especially on the effect towards security behavior does not represent the sole effect of ISC.

Section 2.11.4 reveals that a number of studies have examined the relationships between ATT, NB and SE towards employees' ISP compliance intention (INT). Table 2.10 shows the relationships between ATT, NB and SE towards the main DV in six selected ISC studies. Interestingly, no study has examined the relationships. This suggests that currently no ISC study has examined these particular relationships even though the relationships are widely tested in the literature. Nevertheless, two studies are able to provide empirical findings on the relationships between ATT, NB and SE towards intention of particular behaviors. Flores and Ekstedt (2016) used intention to resist social engineering whereas Dugo (2007) used intention to ISP violation as the main DV of interest. Consistent with security behavior literature, in general, both studies found significant relationship of these three behavioral factors towards employee's security behavioral intention. However, there are slight different interesting findings to be noted. Among the three factors, NB is the strongest predictor in Dugo (2007), whereas in Flores and Ekstedt (2016) NB is the weakest. On the other hand, ATT is the strongest predictor in Flores and Ekstedt (2016) but the weakest in Dugo (2007). Despite the opposite direction of main DVs, another justification on this mixed findings could be explained by the differences of other constructs used in these two research models. Instead of using ISC, these two studies also used different constructs in their models, which in turn affected regression results.

Table 2.10 Relationship between ATT, NB and SE towards an Main Dependent Variable of Interest in Selected Studies

		Path Coefficient, β with Dependent Variable		
Study	**Main Dependent Variable Used**	**ATT**	**NB**	**SE**
Dugo (2007)	Intention to Violate ISP	β=0.201*	β=0.471**	β=0.148**
D'Arcy & Gwen Greene (2009)	Security Compliance	NA	NA	NA
D'Arcy & Greene 2014)	ISP Compliance Intention	NA	NA	NA
Alkalbani et al. (2015)	Information Security Compliance	NA	NA	NA
Parsons et al. (2015)	Attitude towards Compliance	NA	NA	NA
Flores & Ekstedt (2016)	Intention to Resist Social Engineering	β=0.57***	β=0.08***	β=0.09***
*p < 0.1 **p < 0.05 ***p < 0.01 ****p < 0.001 NA – Not Applicable/not examine the relationship				

Analysis of findings on the relationship between ISC and particular constructs of security behavior could also be explained by using R^2 values. Table 2.11 shows R^2 values of endogenous constructs from all selected studies in relation to relationships between ISC and ATT, NB and SE as well as the main DVs employed in the six studies. In the table, the constructs that appear in brackets represent exogenous constructs involved in the regression. Since R^2 value is the variance of endogenous constructs explained by exogenous constructs, therefore different sets of exogenous constructs produce different regression results. Table 2.11 clearly shows that solid findings are lacking on the sole effect of ISC towards security behavior in terms of ATT, NB and SE and other dependent variables of security behavior. From the six selected studies, only two security behavioral constructs having absolute proportion of variance that explained solely by ISC construct, which are NB by Dugo (2007) and Flores and Ekstedt (2016); and another one is main DV of Security Compliance by D 'Arcy and Greene (2009). This means that several more security behavior constructs were not exclusively explained by ISC.

Besides that, Table 2.11 also shows slight mixed findings. The proportion of variance explained in NB by ISC in Dugo (2007) is weak whereas it is stronger in Flores and Ekstedt (2016). According to Cohen (1988), R^2 values of 0.26, 0.13 and 0.02 are considered as substantial, moderate and weak respectively. Therefore, these two findings could not provide strong justification to conclude the actual effect of ISC towards security behavior. Moreover, while there are differences in terms of ISC concept, the findings from both studies also could not suggest the clear dimensions of ISC in influencing the particular behavior factors. As shown in Table 2.9, both studies using unidimensional construct of ISC.

As from theoretical perspective of TPB that Intention is predicted by ATT, NB and SE, current ISC studies also could not provide strong empirical findings on these relationships. In Table 2.11, although studies by Dugo (2007) and Flores and Ekstedt (2016) show R^2 for main DVs explained by three behavioral factors, both main DVs are not exactly the intention to comply with ISP. As depicted previously in Table 2.10, study by Dugo (2007) used Intention to Violate ISP and Flores and Ekstedt (2016) used Intention to Resist Social Engineering. Although these two variables basically represent intention, which is consistent with TPB context, the exact variable of ISP Compliance Intention will provide more clear findings as Padayachee (2012) defines that information security behavior is a set of core information security activities that have to be adhered to by end-users to maintain information security as defined by ISP. Furthermore, the findings could not provide particular aspects of ISC establishment since ISC concept used in both studies are unidimensional construct. This issue is discussed in the next section. As a conclusion, no solid empirical findings is available to explain and support ISC influence towards employee's ISP compliance behavior particularly in terms of ATT, NB and SE as well as towards the main dependant variable of behavioral intention as posited by TPB.

2.13.2 Dimensions in Establishing a Positive ISC

As discussed in previous section, only six studies empirically examine the relationship between ISC and security behavior from eight selected databases published between 2000 until 2017. This number is decreased significantly when considering the findings that could be used as guidelines to establish a positive ISC in the organization. Obviously, a study should use particular dimensions to represent ISC concept. This is

because these dimensions represent aspects or elements of ISC. For example, D'Arcy and Greene (2014) used three dimensions, which are Security Communication (COM), Top Management Commitment (TMC) and Computer Monitoring (MON) to represent the ISC concept in their study. They pointed out these three dimensions represent information security efforts that could be carried out by practitioners in cultivating organizational ISC. Therefore, the findings from the studies applying ISC as a multidimensional construct could provide clearer findings on the aspects of ISC establishment compared to studies that used ISC as unidimensional construct.

Unfortunately, there is a lack of studies that conceptualized ISC based on particular dimensions in examining its relationship towards security behavior. Referring to Table 2.9, only three studies were categorized in this category including D'Arcy and Greene (2009); D'Arcy and Greene (2014); and Alkalbani et al. (2015). In conceptualizing ISC, D'Arcy and Greene (2009) used two dimensions, which are Top Management Commitment (TMC) and Security Communications (COM). In their next study (D'Arcy & Greene, 2014), they used three dimensions by adding one more dimension, which is Security Monitoring (MON) into the existing two. On the other hand, Alkalbani et al. (2015) employed three ISC dimensions, which two of them are totally different from D'Arcy and Greene (2014). As depicted in Table 2.9, instead of using TMC as in D'Arcy and Greene (2009) and D'Arcy and Greene (2014), Alkalbani et al. (2015) used two dimensions of Information Security Awareness (ISA) and Accountability (ACC) which are very different dimensions compared to D'Arcy and Greene (2009) and D'Arcy and Greene (2014). While these additional and different dimensions provided new insights on the concept of ISC, it also leads to a new issue in terms of determining the most appropriate dimensions in representing ISC concept. Consequently, since these dimensions represent information security aspects and guidelines on establishing ISC, this scenario has created some problems for practitioners in selecting the suitable guidelines to be applied in their organization. Moreover, no mutual agreement on the definition and number of dimensions representing ISC concept are available in the literature (Alnatheer, 2015; Lopes & Oliveira, 2014). Therefore, all these arguments and issues suggest that there is still lack of clear and holistic guidelines of ISC cultivation in improving security behavior available in the literature.

Table 2.11 Coefficient of Determination, R^2 of Particular Security Behavioral Constructs in Selected Studies

Study	Attitude (Exogenous constructs involved)	Normative belief (Exogenous constructs involved)	Self-Efficacy (Exogenous constructs involved)	Main Dependent Variable (Exogenous constructs involved)
Dugo (2007)	0.228 (ISC, Perceived punishment certainty, Perceived punishment severity, Organizational commitment)	0.022 (ISC)	NA	0.417 (Attitude, Normative Belief, Self-Efficacy)
D'Arcy & Gwen Greene (2009)	NA	NA	NA	0.31 (ISC)
D'Arcy & Greene (2014)	NA	NA	NA	0.45 (ISC, Job Satisfaction, Perceived Organizational Support)
Alkalbani et al. (2015)	NA	NA	NA	0.48 (Top Management Commitment, Accountability, Information Security Awareness)
Parsons et al. (2015)	NA	NA	NA	NA
Flores & Ekstedt (2016)	0.19 (ISC, Information Security Awareness)	0.21(ISC)	0.24 (Information Security Awareness)	0.42 (Attitude. Normative Belief, Self-Efficacy)

2.14 ISC-Related Study in Malaysian Context

Based on review in Section 2.13 and its sub-sections, basically there is a lack of studies has been conducted to empirically examine the relationship between ISC and ISP compliance behavior and none of the selected studies in the review conducted in the context of Malaysian organization. However, there are still number of ISC-related studies that addressing particular issues of ISC in relation to organizations and employees in Malaysia. Since this research targets Malaysian public universities to validate the model, the following sections explore and discuss ISC-related studies in Malaysia.

2.14.1 Studies of Information Security Culture in Malaysia

Table 2.12 shows summary of ISC related studies conducted in Malaysian context. ISC study in Malaysia commenced by Zakaria (2004). His study provides an overview and justification for conceptual and methodological decisions in investigating the challenges pertaining to ISC cultivation in Malaysian organization. The findings of this study were employed in his next study conducted at Malaysian Administrative Modernization and Management Planning Unit (MAMPU) as case study (Zakaria, 2007). He found that inappropriate security practices were the most challenging issues in Malaysian organization. This issue has resulted in the increment of security incidents caused by employees or insiders. He attributed the cause to security policy that may not be fully understood or relevant to the actual security practices in an organization. He then suggested that basic assumptions about the insiders should be studied to help ISC development within the organization. As a result, it may turn to help reducing internal security incidents.

Apart from that, most ISC-related studies conducted in Malaysia are for healthcare organization. Hassan and Ismail (2012) in their attempt to study ISC in Malaysian Health Information System (HIS) succeeded in developing a conceptual ISC model based on influencing factors from the literature. This conceptual model consists six factors of Behavioral, Change Management, Information Security Awareness, Security Requirements, Organizational System and Knowledge. However, in Hassan and Ismail (2016), four factors influencing ISC in healthcare informatics such as

Security Behavior, Security Value, Security Awareness, and Enforcement of Security Policy were introduced.

The study of ISC in healthcare organization was continued by Hassan, Ismail, and Maarop (2013) and Hassan, Ismail, and Maarop (2014). Hassan et al.'s (2013) study produced a conceptual model to investigate the role of key resistance factors in knowledge sharing towards ISC; whereas, Hassan et al.'s (2014) constructed a conceptual model to investigate the relationship between ISC and Knowledge Management in healthcare organization. Meanwhile, Shahri, Ismail, and Rahim (2013) investigated the relationship of ISC with particular aspects. More recently, Hassan et al. (2017) proposed and validated ISC model for healthcare organization. They found that twelve factors may influence information security culture in health informatics environment and most factors were not emloyed in conceptual model in Hassan & Ismail (2012).

Shahibi, Fakeh, and Ali (2012) also developed ISC model based on ISC factors from the literature in examining the factors contributed to information security culture among ICT librarians. In this study, they found that principles, which is ISP as the most significant factor influencing ISC compared to other factors of Organizational Behavior Tier, Culture Level and Security Control. More recently, Masrek (2017) and Masrek et al. (2017, 2018) conducted series of studies to develop ISC model for Malaysian public organization. They discovered six dimensions were significant for ISC concept including management support, policy and procedures, compliance, awareness, budget and technology. Interestingly, factors from these two studies are not the same with those from ISC studies in healthcare organization by Hassan & Ismail (2012) and Hassan et al. (2017) even though healthcare organization is a public organization.

Table 2.12 Summary of ISC Studies in Malaysia

Author	Objective	Findings
Zakaria (2004)	To overview and justify the conceptual and methodological decisions in investigating the challenges pertaining to ISC cultivation in Malaysian organization. MAMPU is the case study.	• Interpretivism paradigm - main strategy in inquiry. • Data collection - questionnaire survey, semi-structured interviews, reviews of information security documents and observations. • Conceptual framework based on Schein's (1992) model of organizational culture - to guide the data collection techniques

Table 2.12 continued

Author	Objective	Findings
Zakaria (2007)	To examine the challenges involved in the development of an information security culture within public sector context in Malaysia focusing on organizational and cultural aspects of information security.	• Inappropriate security practices result in an increase in security incidents caused by insiders. • Security policy may be either not fully understood or irrelevant to the actual security practices. Interpreting the basic can help develop an information security culture within the organization
Hassan and Ismail (2012)	To propose ISC conceptual model to be applied in HIS	Conceptual model of ISC based on factors influencing ISC from the literature. This model will be validated in HIS in Malaysia. The factors are Behavioral, Change Management, Information Security Awareness, Organizational System, Security Requirements, Knowledge
Shahibi et al. (2012)	To investigate the factors that contribute to the information security culture among ICT librarians	The factors are Principles, Organizational Behavior Tier, Culture Level and Security Control. Principles, which is ISP as the most significant factor of ISC
Shahri et al. (2013)	To identify security culture and security awareness as the basic non-technical factors for IS security effectiveness models in the healthcare domain	From relevant literature, the authors developed a conceptual framework for HIS security effectiveness based on Security Culture and Security Awareness
Hassan et al. (2013)	To investigate the role of key resistance factors in knowledge sharing towards information security culture in healthcare organization	Conceptual model consisting key resistance factors was proposed. This model will be tested in selected healthcare organizations in Malaysia
Hassan et al. (2014)	To investigate the relationship between security culture and KM	Conceptual model of relationship between knowledge sharing with ISC. This model will be tested in selected healthcare organizations in Malaysia
Hassan et al. (2015)	SLR to find key factors that affect ISC	Nine factors discovered with security behavior are the most common factors. Other factors are Security Awareness, Top Management, Cultural Differences, Trust, Information Sharing, Security Knowledge, Security Policy and Belief
Hassan & Ismail (2016)	To identify factors influencing ISC in Healthcare Informatics	Security Behavior, Security Value, Security Awareness, and Enforcement of Security Policy
Masrek (2017; Masrek et al. (2017, 2018)	Development of ISC Model for Malaysian Public Organizations	Six dimensions were significant towards ISC concept, which are management support, policy and procedures, compliance, awareness, budget and technology

Table 2.12 continued

Author	Objective	Findings
Hassan et al. (2017)	To validate ISC conceptual model for healthcare organization	Twelve factors influence ISC, which are Security Knowledge (SK); Security Awareness (SA); Security Behavior (SB); Security Policy Enforcement; Security Decision Making Should Rely On Facts And Rationality That Security Is Important (SD); Improving Information Security Requires A Long-Term Commitment (SLT); Proper Security Systems And Process Motivate Employee To Adhere To Security Policies And Procedure (SESP); Organizations Must Make Continuous Changes To Improve Information Security (SCH); Employee Should Be Involved In Improving The Overall Organization's Information Security (SBI); Collaboration And Cooperation Are Necessary For Effective Information Security (SCC); A Shared Security Vision And Shared Security Goals Are Critical For Effective Information Security (SCV); Information Security Needs Should Be Determined By External And Internal Requirements (SEI); Top Management Commitment (TMC).

2.14.2 Gaps in ISC Studies in Malaysia

Based on review of ISC related studies in previous section, clearly many more areas and perspectives should be explored and studied to obtain profound understanding of ISC concept and utilizing the benefits that could be provided by ISC. Table 2.13 shows areas explored, compared with emerging issues need to be examined further.

Firstly, in relation to factors or dimensions used in ISC model of particular Malaysian organizations, it was discovered that most studies produced different sets of ISC factors even for the same type of organization. For example, ISC model or concept for healthcare organization in Hassan et al. (2017); Hassan and Ismail (2016); and Hassan and Ismail (2012) produced three sets of different factors as depicted in Table 2.12. This scenario is consistent with review in Section 2.5.3 and Section 2.6.1 that found various sets of different ISC dimensions were discovered in the literature. In wider perspective, this issue becomes more obvious. Recent studies by Masrek (2017); and Masrek et al. (2017, 2018) found that six dimensions including management support, policy and procedures, compliance, awareness, budget and technology were

significant towards ISC in public organization. However, the term public organization in Malaysia actually applies to many types of organization including healthcare consisting public hospitals and clinics. Therefore, the factors found in Masrek (2017) and Masrek et al. (2017, 2018) somehow should be the same with Hassan et al. (2017); and Hassan and Ismail (2012).

The issue of ISC model based on set of particular dimension needs to be addressed properly. Clearly, a basic model based on dimensions or factors that applicable for all organization types should be constructed. One of the reasonable starting points is to adopt the same and basic key concept applicable to all organizations such as organizational culture by Schein (1999). Apart from being widely accepted in ISC literature, this concept is general and applicable to all organization types. In fact, ISC is a subculture of OC (Alnatheer & Nelson, 2009; Reid et al., 2014; Schlienger & Teufel, 2003b). Therefore, ISC factors or dimensions formulated based on this concept could be applied and referred as basic model for all types of organization. A series of comprehensive studies should be conducted in narrowing this gap and issues so that a strong foundation of ISC factor and conceptual model can be developed particularly in the context of Malaysian organization.

Secondly, this conceptual model needs to be validated in various domains and different sizes of organization. This is due the fact that culture of information security is found to be different according to organization domain (Ayyagari & Tyks, 2012; Main et al., 2009) and organization size (Dojkovski et al., 2007b; Kuusisto & Ilvonen, 2003; Lopes & Oliveira, 2014; Main et al., 2009; Williams, 2009b). The investigation on these ISC aspects will provide richer outputs and findings towards particular culture of information security in various types and size of organizations in Malaysia.

Thirdly, study pertaining to the challenges faced by Malaysian organizations in cultivating ISC is last carried out in 2007 by Zakaria (2007). Hence, latest study must be conducted to find new possible challenge since it has been almost ten years since previous study. Furthermore, many changes have happened to organizations from various aspects.

Table 2.13 Areas of ISC Studies and Issues to be Further Explored

No.	Areas of ISC studied	Findings	Gap/issues
1.	Factor of ISC	Factors influencing ISC in healthcare organization (Hassan & Ismail, 2012, 2016; Hassan et al., 2017) and public organization (Masrek, 2017; Masrek et al., 2017)	- Some factors are still not empirically tested - Different factors of ISC concept for the same type of organization
2.	Conceptual and Empirical models of ISC	- Conceptual model (Hassan and Ismail, 2012) - Empirical model (Shahibi et al., 2012), (Masrek, 2017; Masrek et al., 2017, 2018)	- Still not validated (conceptual) - Different factors of ISC model for the same type of organization
3.	Conceptual models of relationship between ISC and particular aspects	- Relationship between ISC and security awareness with IS security effectiveness (Shahri et al., 2013) - Relationship between knowledge sharing towards ISC (Hassan et al., 2013) - Relationship between knowledge sharing with ISC (Hassan et al., 2014)	Still not validated (conceptual)
4.	Domains of Organization have been examined	Health, Public Organization, Library	- Academic, GLC, different type and size of organization should have different type of ISC - Need for a reference model
5.	Challenge in ISC	Inappropriate security practices (Zakaria, 2007)	The study conducted in 2007

Another important area needs to be studied is current status pertaining to perceptions and awareness of Malaysian employees toward ISC concept and implementation in Malaysia. An indication of these aspects will show how Malaysian organizations have so far reacted to ISC. These findings then could be applied as references for academicians and starting point for future studies.

Finally, Table 2.13 indicates studies on ISC relationship towards particular aspects of knowledge sharing, knowledge management and security system

effectiveness have yet to be empirically tested. Whilst, it is important to get these empirical results and findings, ISC relationship towards other aspects should also be explored as investigated in other countries and cultures. Among these aspects including information security behavior (Alfawaz et al., 2010), ISP compliance behavior (Alkalbani et al., 2015; D'Arcy & Greene, 2014; D'Arcy & Greene, 2009) and ISC validation and assessment applications (Alhogail, 2015a; Martins and Da Veiga, 2015).

In summary, many more ISC aspects in Malaysian organization's context need to be explored and studied. Based on current available studies, the most important aspect is to develop ISC conceptual model based on general concept of organizational culture so that it could be referred by all types of Malaysian organization. This model then needs to be validated to ensure its applicability towards each type of organization. Despite could be used as guidelines for establishing ISC in each type of organization, the model could also represent as a reference model for Malaysian organization since one of the prominent key factors of ISC is national culture (Alnatheer, 2014; Connolly & Lang, 2013; Govender et al., 2016). This model could be referred by academicians in exploring more possibilities and findings related to ISC studies.

2.15 Information Security in Malaysian Public Universities

In Malaysia, generally there are two types of Higher Educational Institutions (HEIs), which are public HEIs and private HEIs. Until December 2017, according to MOHE, public HEIs consist of 20 public universities; whereas, there are more than 400 of private HEIs that consist of universities, university colleges, colleges and overseas' university branch campuses. The main difference between these two types of HEI is in term of funding. Public universities are considered as government institution funded by government; whereas private universities are self-funded or a subsidiary company of bigger corporations. Since all public universities are funded by the government, they basically are bigger institutions than private HEIs. They have more courses and students. Therefore, they have more ICT facilities to fulfil the requirement of their organizations. Considering that ISC is different according to organization's type and size, basically these two types of HEI also have different ISC.

In terms of Information Scurity Policy (ISP), all Malaysian public universities adopting "Dasar Keselamafan ICT" or DKICT provided by the Malaysian goverment

under MAMPU. The reason is that they are one of the organization under Malaysian public sector and should follow all the requirements set by the government īncluding protection of the iinformation assests. As discusses above, all the assets and funds are provided by the goverment. Therefore they should follow and comply to all the policies including DKICT as provided by MAMPU.

As for the practices and isues of information security for this sector, there are few studies addressed these matters. Ismail, Masrom, Sidek, and Hamzah (2010) conducted a study to propose a framework of information security in Malaysian public universities. They developed the framework based on several standards of information security framework such as MyMIS, ISO/IEC 27001, COBIT and COSO. Interviews were conducted to IT-expert staff and personnel in-charge of developing Information Security framework for selected public universities in Malaysia to determine the components of HEIs framework. They found that there are five components of HEI information security framework, which are Information Security Policy, Risk Management, Access Control, Awareness Program and Training and Compliance. In this study, the researchers also conducted a survey to validate these components and found that all components were significant to the framework.

Although the study by Ismail et al. (2010) provided important guidelines to the implementation of information security in Malaysian public universities, it did not specifically discuss ISC concept and how ISC influences employees' ISP compliance behavior. As such, in Malaysian public university settings, it remains unclear of what ISC is, and what are the components required to establish ISC that would effectively guide employees' security behavior. In addition, the findings were based on perspective of IT-related employees only. Since security issues involved all types of employees, they should be involved in producing a framework applicable to all types of employees throughout the organization. The same scenario is also applicable in assessing ISC in an organization. According to Cardoso et al. (2017), those responsible for IT security in organization should involve all employees in security culture assessment so that more complete view of existing perception could be constructed.

Apart from that, previous study conducted by Sharif, Ismail, and Masrom (2007) towards students and non-IT staff in a Malaysian public university found that level of user awareness, understanding and acceptance of ISP were not sufficiently high and

more concern was required for the implementation of information security. However, more recent study by Hamid and Zeki (2014) found that Information Security Awareness (ISA) among students was high but still demanded stronger Security Education, Training and Awareness (SETA) programs. This is consistent with Olusegun and Ithnin's (2013) study which developed and implemented an information security awareness program to examine and educate awareness of university's employees towards the importance of information security. All these information security issues and requirements clearly are indicators that this sector actually needs to establish ISC to have more holistic approach of organizational effort. The reason is that security measures, ISP and awareness program are among the elements or dimension in ISC (Chen et al., 2015). In fact, Hina and Dominic (2016) claimed this sector is still far behind in adopting ISC and this is critical because Ayyagari and Tyks (2012) have demonstrated and discussed how lack of ISC resulted in serious disaster to a university.

In addition, since public universities are naturally promoting teaching, learning and research, they operate towards more open culture of "information sharing" (Ayyagari & Tyks, 2012; Hina & Dominic, 2017) with all stakeholders and customers compared to other sectors such as banks or government agencies. Educational sector such as public universities usually keep a large amount of information for open access to faculty, staff, student and public usage (Hina & Dominic, 2016). Their network services and applications should also support variety of sharing activities and virtual computing resources (Rezgui & Marks, 2008). The network design that support all these features tend to be user friendly and open to fast delivery; thus, making it more vulnerable to security breaches (Hina & Dominic, 2017). Therefore, smarter strategies of information security mechanisms and management must be in place to balance between the information services given to users with the protection of information assets.

2.16 Chapter Summary

This chapter discusses and analyzes related issues in both area of literature, which are ISC and ISP compliance behavior. It was found that significant gaps were discovered in ISC concept particularly in terms of comprehensiveness and consistency of dimensions used to represent the concept. However, the review revealed that Organizational Culture by Schein (1999) was the most widely accepted concept to

conceptualize ISC. Although Van Niekerk and Von Solms (2006) adapted this concept to develop their ISC framework and added security knowledge as additional level, specific and measurable dimensions for each level produced are still lacking.

Theory of Planned Behavior (TPB) was found to be the most significant theory and its main constructs were the most significant predictors for ISP compliance intention. There is also lack of convincing empirical findings on the relationship between ISC and ISP compliance behavior applicable as guidelines for establishing a positive ISC in guiding employees' information security behavior in an organization particularly in educational sector. All these findings are used as justifications for the development of research model and hypothesis in the next chapter.

CHAPTER 3

RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

3.1 Introduction

Previous chapter found that comprehensive empirical findings to conclude actual relationship between ISC and ISP compliance behavior is still lacking. No mutual agreement on factors or dimension of ISC concept is found. This implies that currently there is a lack of ISC model for employees' ISP compliance behavior has been produced. Thus, suggesting more researches are required to establish ISC model that could be referred in understanding the concept of ISC as well as to be used in assessing and cultivating a positive ISC in the organization.

This chapter presents the research model and hypotheses of this research. Following this introduction section, section two justifies theoretical frameworks used to form the research model. Section three discusses the formulation of dimensions to represent the ISC concept followed by discussion of the overall ISC concept based on formulated dimensions in section four. Section five discusses conceptual framework and hypotheses proposed in this research. Finally, summary of this chapter is presented in section six.

3.2 Theoretical Framework

This study uses Organizational Culture by Schein (1999), Theory of Planned Behavior (TPB) (Ajzen, 2005) and layered approach ISC framework by Van Niekerk and Von Solms (2006) as theoretical frameworks and foundations in formulating, representing and linking the concepts ISC with employee's security behavior as illustrated in Figure 3.1. Specifically, Organizational Culture (OC) concept by Schein (1999) together with ISC framework by Van Niekerk and Von Solms (2006) were used

as foundations to formulate dimensions of ISC in this study. As discussed in Section 2.9, ISC framework by Van Niekerk and Von Solms (2006) consiting of four levels and the upper three levels are adopted directly from levels in Schein's OC. Meanwhile, TPB is used to represent employee's ISP compliance behavior that links the relationship with ISC. Furthermore, the main constructs of TPB, which are Attitude, Normative Belief and Self-Efficacy were used to represent an employee's ISP compliance behavior factors that link to his/her ISP compliance intention. The use of TPB as theoretical behavioral framework is consistent with Schein (2004) who recommended to study culture by building models based on deeper and more complex anthropological view.

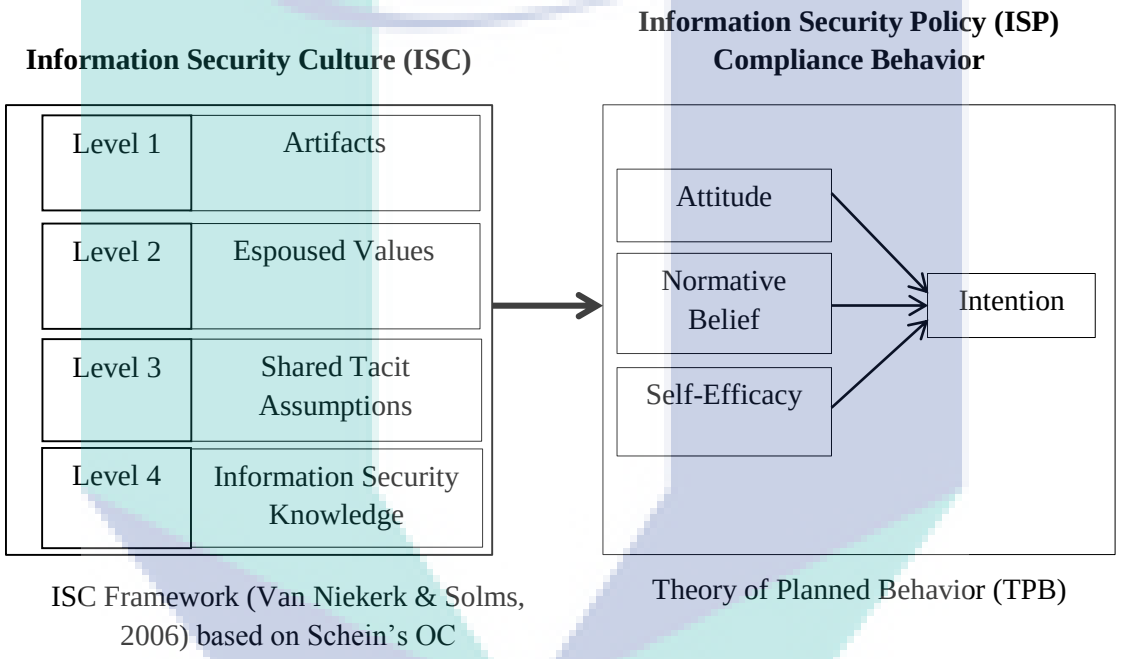


Figure 3.1 Theoretical Framework

As discussed in Section 2.8 (Chapter 2), the most adopted concept in understanding ISC is Organizational Culture (OC) by Schein (1999). This concept consists of three levels, which are artifacts, espoused values and shared assumptions. Van Niekerk and Von Solms (2006) employed these three levels with additional level named Information Security Knowledge to develop their ISC framework. This current research adopted all four levels in Van Niekerk and Von Solms (2006) and all three levels in Schein (1999) as theoretical frameworks to formulate and identify associated dimensions for each level of ISC concept. They also guide and limit the factors involved in each formulated dimensions.

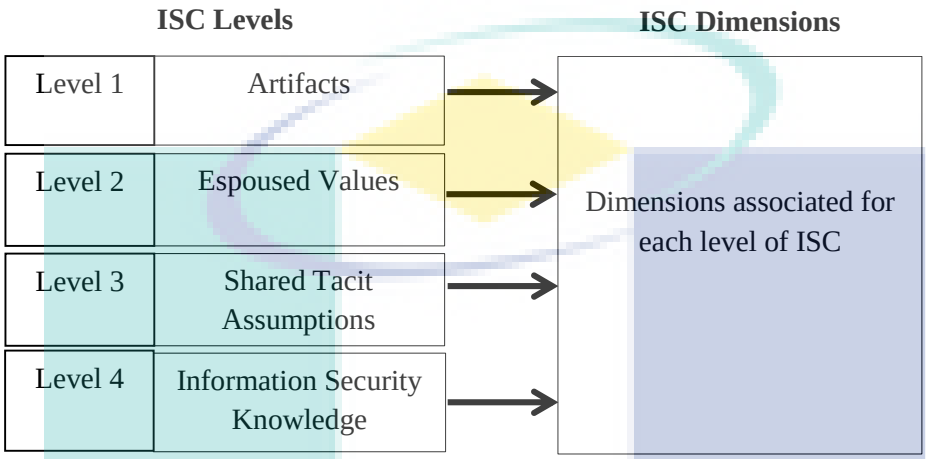
Apart from that, according to Schein (1999), organizational culture helps to guide different employees' behavior as well as to influence what is determined to be acceptable in organizations. Since ISC concept in this research was derived from OC by Schein (1999) and ISC framework by Van Nikerk and Von Solms (2006), it was assumed that ISC is a subculture that could influence employees' security behavior, which is represented by TPB. As security behavior is commonly referred to ISP compliance behavior (Padayachee, 2012), this research proposes that ISC would influence ISP compliance behavior. It is also consistent with Vroom and Von Solms (2004); Eloff and Von Solms (2000); Von Solms (2000); Van Niekerk and Von Solms (2010) who suggested the establishment of ISC will guide and influence employees' behavior to comply with ISP. Refering back to Table 2.2 in Section 2.5 (Chapter 2), all these studies also used both Schein's OC and ISC framework by Van Niekerk & Von Solms (2006) or one of them in conceptualizing their ISC. The next sections discuss all these aspects in detail, which finally propose a conceptual framework for this study.

3.3 Formulation of ISC Dimensions

In this research, ISC framework by Van Niekerk and Von Solms (2006) was adopted as foundation to formulate the ISC dimensions. The reason is this framework was developed using widely accepted concept in information security field, which is Schein's OC. While providing more comprehensive concept based on level approaches, Schein's OC also was successfully used to conceptualize ISC in many ISC-related studies (Kolkowska, 2011) such as in Da Veiga and Eloff (2010); Thomson (2010); and Vroom and Von Solms (2004). Moreover, the use of Schein's OC together with ISC framework by Van Niekerk and Von Solms (2006) in the formulation also enables more comprehensive assessment on all levels (Okere et al., 2012) so that the dimensions formulated will comprehensively covered all aspects of ISC. In other words, this way ensures that all ISC levels were taken into consideration and all ISC levels can be measured by their correspondence dimensions.

The formulation was conducted by using a mapping process from ISC levels into ISC dimensions as illustrated in Figure 3.2. Specifically, the mapping process was conducted based on justification and function of each level in OC (Schein, 1999) and ISC (Van Niekerk & Von Solms, 2006) so that each dimension mapped is a representation of certain level comprised in OC (Schein, 1999) and ISC (Van Niekerk &

Von Solms, 2006). The mapping process of a concept onto particular dimensions to represent ISC concept is not new in this field. Martins and Eloff (2002) also mapped three levels of Organizational Behavior (Robbins, 2001) onto ISC dimensions of their ISC model. The next sections discuss these processes in detail.



ISC Framework (Van Niekerk & Solms, 2006)

Figure 3.2 Mapping Process

3.3.1 First Level - Artifacts

The first level in ISC is the artifacts in the organization. These artifacts are visible and easily spotted by outsider (Schein, 1999, p. 15). Examples of these would be the architecture and decor of the company. In information security context, actual physical security of the organization, such as locked doors, would be an artifact (Vroom & Von Solms, 2004). According to Ngo et al. (2009), artifacts are visible organizational policies and processes based on the expressions of norms and values that affect the behavior of organizational members. Reid and Van Niekerk (2014) suggested that the examples of artifacts would be the architecture and security mechanisms of the company, as well as information security policies and procedures. Since it was clear that this level is related to security countermeasures employed by the organization in dealing with information security, these artifacts were mapped to be represented by two types of information security countermeasures, which are procedural and technical.

In this study, Procedural Countermeasures (PCM) is defined as a security countermeasures that concern with guidelines, procedures and policies set up by the organizations to guide information security matters. Schlienger and Teufel (2002,

2003a) argued that the handbooks, rituals and anecdotes are examples of artifacts which are formed by collective norms and values of organizations. According to Malcolmson (2009), artifacts are procedures that can be seen or touched such as physical environment, processes, procedures and documents. The most obvious examples of PCM are Information Security Policy (ISP) (Chen et al., 2015; D'Arcy, Hovav, & Galletta, 2009) and other policies such as ethical conduct policies. PCM includes all information security procedural practices that must be followed by employees, such as login into a secure company network using a valid account, procedures of scanning external drives and any related procedures to secure information assets.

According to Chen et al. (2015), having formal and documented security policies in place is an initial step to shape security culture in an organization. Many studies have considered policies, procedures, guidelines and ethical codes as important elements in cultivating ISC (Alnatheer, 2012, 2014, 2015; Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015b; Dojkovski et al., 2010; Martins & Eloff, 2002; Shahibi et al., 2012; Von Solms & Von Solms, 2004a). Da Veiga (2015) empirically found that ISC is more positive if the employees read the ISP. This finding proved the impact and significant role of ISP towards ISC in an organization. It is even considered as the best practice in the field of information security management according to regulations and industry standards (e.g. ISO (International Organization for Standardization)/ IEC (the International Electrotechnical Commission) 27001).

Whilst, PCM concerns on procedural aspects, Technical Countermeasures (TCM) are all about technical aspects of information security measures in ensuring the security of information assets in an organization. This TCM is different with the one used in the study of Hovav and D'Arcy (2012). They define TCM as monitoring activities performed by the organizations towards their employees in ensuring security behavior. However, it seems that these monitoring activities could not represent the artifact level because these activities are hidden from the employees. As mentioned earlier, artifacts are visible and easily spotted by outsider (Schein, 1999, p. 15). In this study, this dimension is defined as technical processes conducted to minimize information security risks and these processes are well-known to all employees throughout organization. It is a technical measure implemented by the organization to ensuring confidentiality, integrity and availability of information. It includes access

control technology such as password mechanism and encryption, virus protections and many more technical measures of network security such as firewall and intrusion detection system.

However, these measures and controls depend upon the type of organization itself specifically in terms of size, business nature and criticality of information system. Small organizations with non-financial based business nature and less critical of information systems have different technical measures in terms of technological measures advancement and security control compared to bigger organizations especially financial organizations that have critical information systems. Due to this fact, this dimension depends on the risk assessment and analysis implemented by each organization to decide the adequacy and appropriateness of measures required. Since this dimension concerns more on mitigating the risks of information security, this dimension is named Risk Management (RM) representing artifact level alongside with PCM. While it is an organizational unit that is well known by all employees, it is also visible and easily recognized by outsiders (Schein, 1999, p. 15). Furthermore, it is consistent with Da Veiga and Eloff (2010) who argued that artifacts are evident as a result of information security components implemented such as risk management and policy component.

In this study RM is defined as a process for resolving risk. The process includes risk assessment to define the risk, and risk control to resolve the risk. Information security risks such as the threat of viruses, hackers or natural disasters need to be identified and the control implemented by considering a cost benefit analysis (da Veiga, 2008). The main elements of RM dimensions include risk analysis and assessment (Da Veiga & Eloff, 2010; Oecd, 2002) and these factors also are key factors for ISC (Alnatheer, 2015; Chia et al., 2002b; Dojkovski et al., 2007b; Martins & Eloff, 2002). As a conclusion, level of artifacts were mapped into two dimensions; PCM and RM as shown in Figure 3.3.

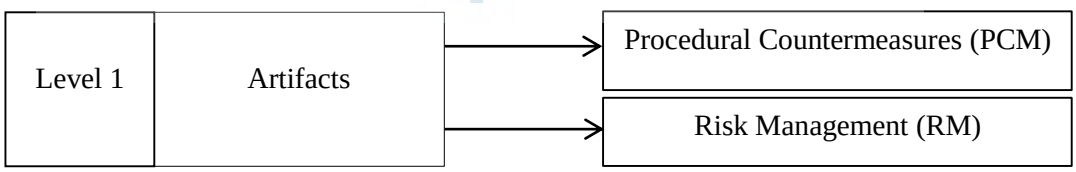


Figure 3.3 Level 1 Mapping

3.3.2 Second Level – Espoused Values

Second level in the ISC framework is espoused values. An organization's espoused values are the "reasons" an organizational insider would give for the observed artifacts (Schein, 1999, p. 17). These are partially visible in the organization and reflect the values of a particular group of the individuals (Schlienger & Teufel, 2002, p. 3). The examples for these include good communication and teamwork (Schein, 1999, p. 17). Another examples are organization's goals, strategies, and philosophies (Shaw, 2012). In an organization that has strong culture, the goals and strategies generally published and well known within the organization (Shaw, 2012).

Although Van Niekerk and Von Solms (2005, 2006) considered this level can be represented by the ISP, in this research, this level is viewed as more suitable to be represented by Security, Education and Training Awareness (SETA) programs as shown in Figure 3.4. SETA are security programs that promotes values espoused in an organizational ISP. SETA are the "reasons" an employee would give for the observed artifacts. Moreover, these information security programs are the strategies originated from top management to reflect values and belief of employees towards information security behavior and practices that in line with the organizational ISP (Vroom and Von Solms, 2004). In other words, the values in ISP are espoused through SETA. The reason is most employees are not aware of ISP so they do not espouse and value this document. Therefore, SETA plays crucial role in espousing desired values related to information security. Stronger SETA in an organization reflects the espoused values of information security. Moreover, ISP is more suitable to represent artifacts rather than espoused value as justified in previous section. ISP is more visible and could be aesily spotted by outsiders rather than SETA. It is also consistent with Huczynski and Buchanan (2007) who argued espoused value level is partially visible and unspoken but can shape the employees' behavior.

Figure 3.4 Level 2 Mapping

SETA is considered as the most important element in cultivating information security culture (Alnatheer, 2012, 2014; Chen et al., 2015; Kajtazi & Bulgurcu, 2013; Kraemer & Carayon, 2005; Ngo, 2008; Da Veiga, 2015a). Schlienger and Teufel (2003b); and Bozic (2012) suggested SETA as a security program that can lead to change and improve the awareness behavior of employees and finally resulting in changing and improving ISC in an organization. Van Niekerk and Von Solms (2005) argued that SETA is required to provide information security knowledge desired by an organization to their employees in their effort to cultivate ISC in the organization. Latest study by Chen et al. (2015) has empirically proved that SETA has significant impact towards ISC. In this current study, SETA is conceptualized to represent level two of ISC level. It is the core of information security programs in ensuring that employees attain the required level of knowledge, skills as well as awareness pertaining to information security; and values of these programs are accepted and espoused by employees throughout the organization.

3.3.3 Third Level – Basic Tacit Assumptions

The third level is basic tacit assumptions. These are hidden, largely unconscious and occur very much at the individual level, and these assumptions are underlying beliefs and values of people in the company (Vroom & Von Solms, 2004). These are normally the original thoughts and beliefs of the founders that have been unconsciously communicated to employees and form the core of organization (Schein, 1999, p. 19). In the context of ISC dimensions, this level was mapped into two subdimensions, which are Top Management Commitment (TMC) and Monitoring (MON) as depicted in Figure 3.5.

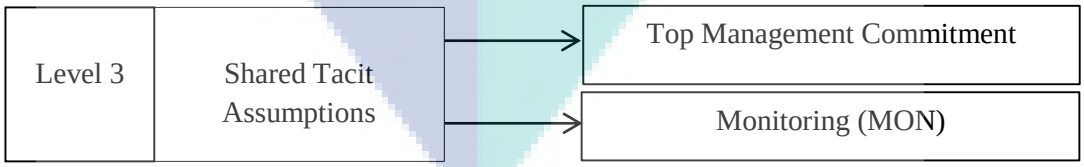


Figure 3.5 Level 3 Mapping

For TMC, this dimension is in the form of employee's belief and trust that top managers are committed to security through their actions related to information security (Dojkovski et al., 2010; Martins & Eloff, 2002). This belief is championed and

communicated by top management to employees throughout the organization. The promotion to cultivate ISC in an organization should be initialized by top management (Van Niekerk & Von Solms, 2005). They need to be aware of and engaged in and supportive of security issues, strategies and policies (Johnson & Goetz, 2007). Top management must give adequate efforts in ISC implementation and these efforts must be understood and accepted by employees throughout the organization. Senior management in the organizations have to demonstrate commitment and dedication for information security (Thomson et al., 2006) and perceive its as important issue and forms a security culture throughout organizational levels (Dutta & McCrohan 2002). In addition, they must act as role models with regard to information security and take initiative in order to be informed about information security topics and develop governance structures for maintaining adequate information security (Lebek, Guhr, et al., 2014). Furnell and Clarke (2005) reasoned that ISC is achievable if the concept is supported by top management.

Many studies on ISC shown that top management commitment is a key factor in fostering and cultivating ISC in the organization (Alnatheer, 2014, 2015; Alnatheer et al., 2012; Kraemer & Carayon, 2005; Martins & Eloff, 2002). This commitment will create strong belief and trust of employees towards ISC implementation in the organization. In this study, this dimension is represented level three of ISC framework which is shared tacit assumptions. These shared tacit assumptions act as a kind of ‘‘filter’’, which affects how individuals will carry out their normal day-to-day activities (Van Niekerk & Von Solms, 2010).

Another dimension mapped from this basic tacit assumptions’ level is Monitoring (MON). Similar to TMC, this dimension regarded as hidden, largely unconscious and occur at individual level. These assumptions are the underlying beliefs and values of people in the company (Vroom & Von Solms, 2004). MON such as security monitoring and audits are usually implemented by the organizations with or without employees realizing it, but somehow, they trust and believe that these countermeasures are implemented to ensure the security of information assets. These shared tacit assumptions act as a kind of ‘‘filter’’, which affects how individual carries out their normal day-to-day activities (Van Niekerk & Von Solms, 2010).

Recent study by Chen et al. (2015) empirically found that Monitoring (MON) has significant impact towards ISC. Literature also indicates this construct is consists of factors or elements of tracking employees' computing activities and performing security audits (Chen et al., 2015; Hovav & D'Arcy, 2012). Monitoring and audits are hidden activities to check and ensure employees' security compliance and behavior. It somehow also measures the trust and belief of employees on information security. In ISC literature, many studies suggested that trust and belief are the key factors of ISC (Ashenden & Sasse, 2013; Merhi, 2014; Ramachandran, Rao, & Goles, 2008; Shahibi et al., 2012; Williams, 2009a).

3.3.4 Fourth Level - Information Security Knowledge

In ISC framework by Van Niekerk and Von Solms (2006, 2010), while still using the same explanation and justifications of levels as OC of Schein (1999), they have justified that a fourth level, which is information security knowledge, is a very important aspect in the context of ISC. The reason is these the levels of corporate culture are the basic aspects/levels in every organization culture. As for ISC, knowledge of information security should be acquired and this knowledge is imperative to provide the effects for each level of three OC levels. Without adequate knowledge of information security, those three levels do not have sufficient knowledge regarding information security and could not form desired and stable ISC. Adequate knowledge of information security posed by an organization ensures the employees behave and practice securely when dealing with information assets (Zakaria, 2006).

Flores, Antonsen, and Ekstedt (2014) argued that these knowledge could be manifested through information security specialists hired to perform activities that increase information security knowledge, or having dedicated units within the organization responsible for those activities. Alhogail (2015a) empirically proved that knowledge has significant relationship with ISC. Knowledge and behavior are two dimensions of human factor in information security. These dimensions are inter-related to each other (Alhogail, 2015a). More recently, Mahfuth et al. (2017) in their systematic review of ISC frameworks found that security knowledge is a key factor of ISC. Lack of knowledge in information security matters leads to a certain misbehavior, intentionally or thorough negligence.

Zakaria (2007) suggested that in adapting the concept of knowledge to information security, security knowledge needs to be externalized in order to be shared and learned by other employees. Information sharing among employees is crucial to overcome any security breach that might occur or prevent them from happening in the first place. Knowledge sharing is important in cultivating ISC to ensure that the knowledge can be transferred, disseminated and distributed to make it available to those requiring it (Hassan et al., 2013). Based on these arguments, Information Security Knowledge (ISK) and Information Security Knowledge Sharing (ISKS) are introduced as two ISC dimensions to be associated with the fourth level of ISC framework by Van Niekerk and Von Solms (2006) as shown in Figure 3.6.

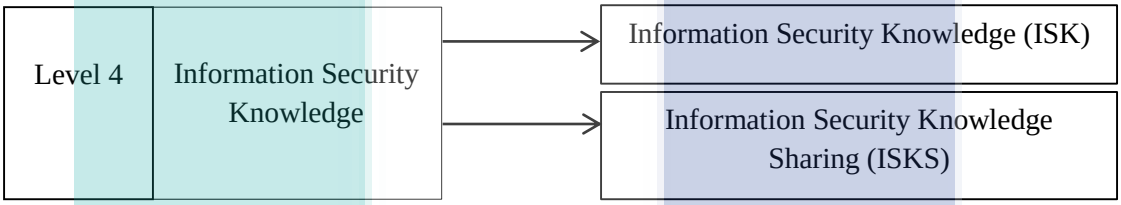


Figure 3.6 Level 4 Mapping

3.4 Information Security Culture based on Seven Dimensions

Figure 3.7 shows the complete result of the mapping process between ISC levels into ISC dimensions. It shows that there are seven dimensions of ISC concept formulated based on levels by Schein's OC and ISC framework by Van Niekerk and Von Solms (2006). In terms of mathematical expression, Equation 3.1 shows general representation of the ISC concept constructed by seven formulated. These findings answer Research Question 1 and achieve Research Objective 1.

$$ISC = \{PCM, RM, SETA, TMC, MON, ISK, ISKS\} \quad 3.1$$

It is worth to note that seven dimensions above do not only cover all levels in ISC framework, they also cover most of ISC key factors in the literature. As discussed in Section 2.4 (Chapter 2), besides the interchangeable use of factor and dimension, the term factor is also used to explain a single overlapped element of ISC, whereas the dimension is used to represent a distinct aspect that group several factors in it.

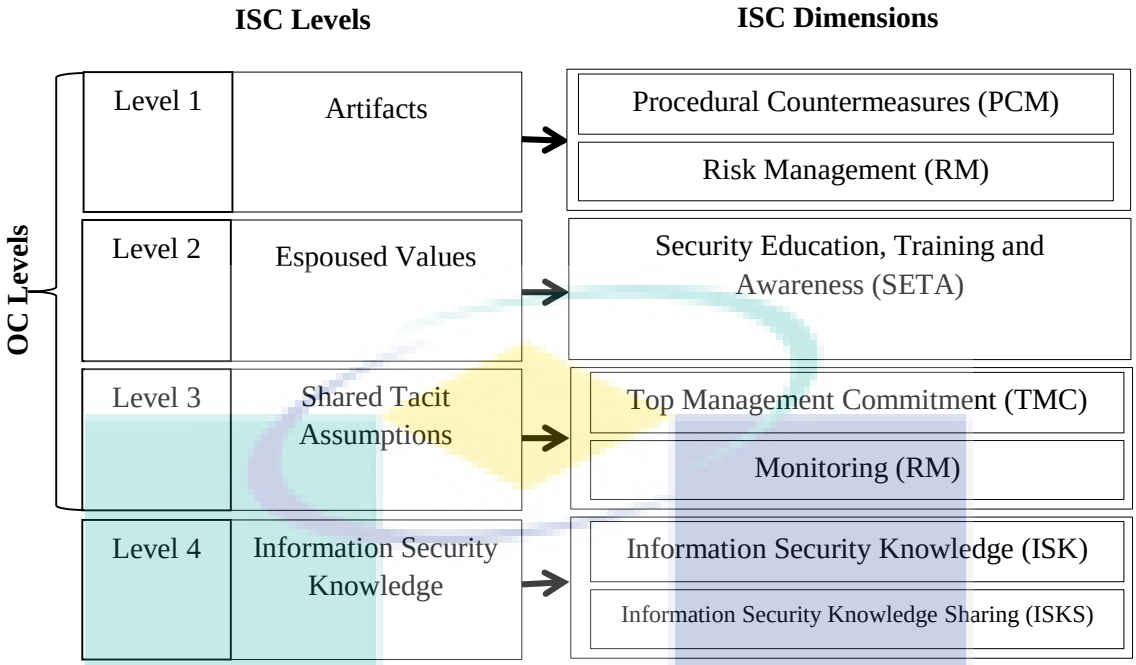


Figure 3.7 ISC based on Seven Dimensions

Table 3.1 shows all seven dimensions with the definitions and its associated factors. All of these factors also are the key factors that found in reviews by Hassan et al. (2015) and Alnatheer (2014) as well as the factor/sub-dimensions identified in Table 2.2 (Chapter 2). Table 3.1 shows that most of these key factors could be allocated in certain formulated dimension. This means that, the seven formulated dimensions did not only comprehensively cover all levels in OC and ISC, these dimensions also covered most ISC key factors available in the literature. This is important because ISC is a complex concept and all important factors should be considered in defining and measuring the concept as argued by Tolah et al. (2017) and Schlienger and Teufel (2003b).

As shown in Table 3.1, all ISC key factors found in current literature were assigned into the associated dimensions respectively based on the definition and functions of each ISC dimension as discussed in Section 3.3.1, Section 3.3.2, Section, 3.3.3 and Section 3.3.4. This allocation also enables the operationalization of each of these ISC factors in the respective dimensions.

Table 3.1 ISC Dimensions, Definition and Its Associated Factors

ISC Dimensions	Definition	ISC Factors Covered
Procedural Countermeasures (PCM)	Refer to all information security countermeasures in the form of procedures and guidelines including security policies and ethical conduct policies to enforce information security in an organization.	ISP, Ethical Conduct Policies
Risk Management (RM)	A process for resolving risk. The process includes risk assessment to define the risk, and risk control to resolve the risk (Hall 1998:5). Information security risks such as the threat of viruses, hackers or natural disasters need to be identified and the control implemented by considering a cost benefit analysis (Adéle da Veiga, 2008).	Risk Analysis, Risk Assessment
SETA	Security Education, Training and Awareness programs in an organization.	Security Awareness, Security Training
Top Management Commitment (TMC)	Commitment shown by top management towards information security issues	Top Management Commitment, Trust, Belief
Monitoring (MON)	Refer to all information security efforts to monitor security compliance and behavior of employees including tracking employees' computing activities and performing security audits in ensuring information security in the organization.	Trust, Belief, Security Compliance, Security Behavior
Information Security Knowledge (ISK)	Adequate knowledge of information, issues, technologies and skills related to information security posed by all levels of organizational culture in order to react accordingly towards all information security matters.	Information Security Knowledge
Information Security Knowledge Sharing (ISKS)	Any forms and activities of communications in helping others to collaborate, so as to solve a problem, establish new ideas, or implement policies or procedures (Wang and Noe, 2010)	Information Security Knowledge Sharing

Procedural Countermeasures (PCM) represented ISP and all other policies such as ethical conduct policies and any visible enforcement relating to the policies. Risk Management (RM) was assigned with Information Security Risk Analysis and Assessment. Security Awareness and Information Security Training factors were assigned into SETA dimension. Monitoring (MON) operationalized factors of Security Compliance, Security Behavior, Trust and Belief. As for Top Management (TMC), this dimension covers Top Management Commitment, Trust and Belief. Although factor of

Trust that originally found by Hassan et al. (2015) is referred to trustful culture in Williams (2008), it is mostly suited to be in level three, which is basic assumption. Trust could not be placed under artifact and shared assumptions because artifacts are something that can be seen, whereas shared assumptions are partially visible. Therefore, associated level for Trust is in shared tacit assumptions, which are hidden, largely unconscious and occur at individual level. Similar to Trust, factor of Belief was allocated in level three since this level is about employees' belief regarding information security as discussed in Van Niekerk and Von Solms (2006); Shahibi, Rashid, Wan Fakeh, Dollah and Ali (2012). Finally, dimensions of Information Security Knowledge (ISK) and Information Security Knowledge Sharing (ISKS) were directly covered and assigned with factors of Security Knowledge and Information Sharing respectively.

3.5 Conceptual Framework

Figure 3.8 shows conceptual framework for this research. Based on theoretical framework in Section 3.2, the multidimensional concept of ISC based on seven dimension was integrated with the most significant theory in ISP compliance behavior literature, which is TPB to form the relationship between these two theoretical paradigms. Based on mathematical expression in Equation 3.1 that form the ISC concept, the complete mathematical representation for this relationship is express in Equation 3.2. The adoption of TPB enables more thorough examination on the influence of ISC towards an employee's security behavior in order to get more deep understanding on the relationship, as behavior is a major concern in information security. Furthermore, ISC is human-centric view which takes into account behaviors and attitudes as well as the underlying system of norms and values (Teufel & Teufel, 2015).

$$Conceptual\ Framework = \{ISC(PCM, RM, SETA, TMC, MON, ISK, ISKS) + TPB(ATT, NB, SE, INT)\} \quad 3.2$$

In general, the conceptual framework shows how ISC based on seven dimensions influences an employee's ISP behavior factors of Attitude (ATT), Normative Belief (NB) and Self-Efficacy (SE), which in turn influence his/her ISP

compliance intention (INT). Specificallly, the seven dimensions of Procedural Countermeasures (PCM), Risk Management (RM), Security Education, Training and Awareness (SETA), Top Management Commitment (TMC), Monitoring (MON), Information Security Knowledge (ISK) and Information Security Knowledge Sharing (ISKS) were the aspects and efforts to be implemented in establishing a positive ISC.

As discussed Section 2.13.1, although few studies have empirically examined the relationship between ISC and ISP compliance behavior, some issues arise due to the disparity in conceptualizing ISC concept. Furthermore, there are many more key factors and dimensions of ISC were not involved in those studies. In this study, ISC was conceptualized as a multidimensional construct forming by seven constructs of PCM, RM, SETA, TMC, MON, ISK and ISKS based on widely accepted concepts of OC and ISC. Whilst, this conceptualization enables more thorough examination on the ISC concept and its relationship with ISP compliance behavior, it also provides more conclusive and clear findings. The next sections discuss the conceptualization and operationalization of ISC as well as research model and hypotheses in detail.

3.5.1 Conceptualization and Operationalization of ISC as Multidimensional Second-Order Construct

Key requirement for defining and operationalizing multidimensional constructs is that they should be derived from theory and the theory should indicate the number of (sub) dimensions and their relationship to the higher-order construct (Johnson, Rosen, Chang, Djurdjevic, & Taing, 2012; Mackenzie, Podsakoff, & Podsakoff, 2011; Polites, Roberts, & Thatcher, 2012). Based on the literature review on ISC concepts in Chapter 2 and formulation of ISC dimensions in Section 3.3 and its sub-sections, this research conceptualized and operationalized ISC concept as a multidimensional second-order construct that has formative relationship with seven new formulated dimensions of reflective first-order constructs.

The formulation of ISC dimensions based on OC concept (Schein, 1999) and ISC framework (Van Niekerk & Von Solms, 2006) produced seven dimensions of PCM, RM, SETA, TMC, MON, ISK and ISKS to represent the ISC concept. In other words, ISC is a multidimensional concept consisting of seven dimensions of PCM, RM, SETA, TMC, MON, ISK and ISKS.

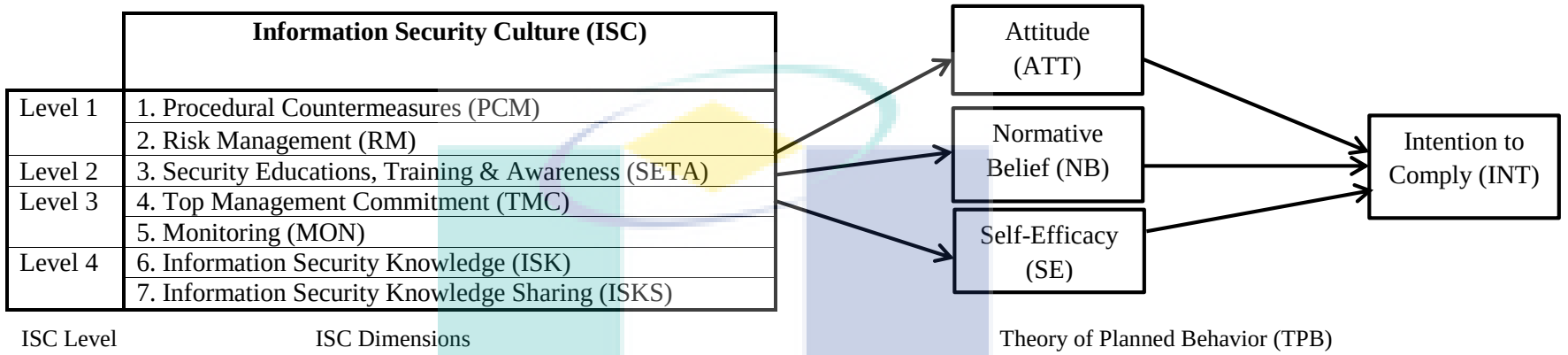


Figure 3.8 Conceptual Framework of Dimension-based ISC Model for ISP Compliance Behavior

Section 3.4 reveals these dimensions also covered almost all ISC key factors in current literature. Thus, this suggests that ISC is a multidimensional construct consisting of seven latent constructs. Each of these constructs or dimensions represents one clearly defined aspect of content domain of the overarching concept or construct (Polites et al., 2012). Prior study by D'Arcy and Greene (2014) also conceptualized and operationalized ISC as multidimensional construct consisting of three latent constructs of Top Management Commitment, Security Communications and Computer Monitoring. These latent constructs are the indicators of ISC construct. According to Polites et al. (2012), constructs are described as multidimensional when their indicators are themselves latent constructs. Therefore, it is clear that ISC is a multidimensional construct.

Although these dimensions are conceptually distinctive, at more abstract level, each can be viewed as describing a different facet of the overall ISC construct (Jarvis, MacKenzie, & Podsakoff, 2003; Law & Wong, 1999; Polites et al., 2012). These seven dimensions form ISC construct, suggesting that the relationship between ISC construct with its lower order constructs is formative similar to prior study by D'Arcy and Greene (2014). This type of relationship is also referred to as aggregate by Polites et al. (2012). An aggregate construct 'combines or aggregates specific dimensions into a general concept', with the relationships flow from dimensions to construct (Edwards, 2001).

Since among the research objectives is to focus on the conceptualization and validation of ISC, this operationalization enables more attention and investigation to the construct. Petter, Straub, and Rai (2007) suggested that a complex construct that is the main topic of study deserves to be modelled as a multidimensional construct to permit a more thorough measurement and analysis. It is consistent with Hair et al. (2014) that stated decision for the relationship between first-order construct and second-order construct depends on theoretical/conceptual reasoning and goal of the analysis. While it was strongly supported in literature that the seven dimensions form the ISC concept, the formative relationship between first-order and second-order meets the objective of this research, which is to validate these dimensions in contributing to the underlying concept of ISC.

In addition, Polites et al. (2012) suggested that if a complex concept is the focus of the study, it is generally best to create a measurement model with all the critical

conceptual distinctions, because it is important to thoroughly test and evaluate the construct. MacKenzie, Podsakoff, and Jarvis (2005) observed that multidimensional second-order constructs are useful when a greater specificity of understanding is wanted in understanding a theoretical construct. Siponen and Vance (2010) suggested that whereas two or three measurement items might suffice to define a construct of peripheral interest, a multidimensional construct allows researchers to develop items that describe a construct in terms of multiple sub-constructs and bringing the nature of the construct into sharper relief.

This way of conceptualization and operationalization enables the researchers to theorize about and evaluate the influence of the higher-order construct (e.g., one set of relationships), rather than the influence of its dimensions (e.g., five sets of relationships) on a dependent variable (Polites et al., 2012). Therefore, it is clear that this research approach is consistent with the goal of this study, which is to specifically investigate the influence of ISC concept on employees' ISP compliance behavior rather than its dimensions. Furthermore, this conceptualization and operationalization enable proper way to investigate the effects of a construct measured by several related constructs or factors (Wright, Campbell, Thatcher, & Roberts, 2012) as conducted by McKnight, Choudhury, and Kacmar (2002) in conceptualizing and operationalizing Trust construct in their study. In the context of this study, this operationalization enabled theory development on the relationship between complex concept of ISC with employee's information security behavior in broader perspectives (Law, Wong, & Mobley, 1998; Wong, Law, & Huang Guo-Hua, 2008).

In summary, this research modelled ISC as a Type II second-order construct (Jarvis et al. 2003), a second-order construct that is formatively composed of reflective sub-constructs. A construct composed in this manner is useful "when multiple sub-constructs and measurement items are necessary to fully capture the entire domain of the construct" (Petter et al. 2007 p. 627). It is also useful in structuring a complex formative construct with many indicators into several sub-constructs (Becker et al., 2012). This fact is consistent and applicable to ISC concept because of the variety and complexity of ISC dimensions identified in prior ISC studies. A formative model is appropriate in this case because the seven ISC dimensions are theoretically independent and their joint effect can be examined at second-order construct level. According to

Hair et al. (2014), formative relationships between Lower-order Constructs (LOCs) and Higher-order Construct (HOC) reveal relative contribution of each LOC in explaining HOC. It enables the examination of impact of each dimension towards ISC. This conceptualization contributes to theoretical conciseness and clarity. Furthermore, it makes the model more parsimonious (Hair et al., 2014).

3.5.2 The Role of ISC towards Employee's ISP Compliance Behavior

According to Schein (2004), culture is "a set of structures, routines, rules, and norms that guide and constrain behavior" (p. 1). It influences how people think and feel as well as how their act, and it provides meaning and predictability in their daily life (Schein, 1999). Culture is one of the most powerful factors to shape human behavior. As discussed in Section 2.8 (Chapter 2), Schein (1999) conceptualized organizational culture as consisting of three levels, which are of artifacts, espoused values and shared assumptions. Van Niekerk and Von Solms (2006) then adopted this concept to develop their ISC framework and added ône more level of knowledge as the fourth level. As discussed in Section 3.3 and Section 3.4, this research formulates seven dimensions based on each level in ISC framework by Van Niekerk and Von Solms (2006) to represent ISC concept. These seven dimensions also represent significant principles, activities and programs in establishing ISC in an organization including public university in Malaysia. Most of these dimensions are presence in the information security framework in Malaysian public university by Ismail et al. (2010).

Drawing from the concepts of Schein's OC and ISC framework by Van Niekerk and Von Solms (2006), this study proposed that culture of information security (ISC) based on seven formulated dimensions would influence employees' behavior towards adhering to ISP established in the organization. As discussed in Section 3.2, while OC could guide behavior in the organization, ISC is a subculture that would influence employees' security behavior. This is consistent with most studies that used Schein's OC or ISC framework by Van Niekerk and Von Solms (2006) in ISC conceptualization.

According to Kolkowska (2011), common assumption of most ISC studies (i.e. Da Veiga & Eloff, 2010; Schlienger & Teufel, 2003a; Vroom & Von Solms, 2004) is that the cultivation of ISC will change employees' security behavior and values so that they comply with organizational security policies and rules. Recently, Glaspie and

Karwowski (2018) argued that most researches highlighted that a positive ISC can increase ISP compliance. Specifically, information security scholars suggested that the establishment of a positive of ISC will influence security behavior of employees (Alhogail & Mirza, 2014a; Da Veiga & Eloff, 2010; Van Niekerk & Von Solms, 2010) particularly in improving ISP compliance in the organization (Da Veiga & Martins, 2015a; Martins & Da Veiga, 2015a; Vroom & Von Solms, 2004).

As discussed in Section 2.11.8 (Chapter 2), consistent with Sommestad et al. (2017); Lebek, Uffen, et al. (2014), the most common and significant theory in explaining ISP compliance behavior is TPB (Sommestad et al., 2017). This theory has three main behavioral factors, which are Attitude (ATT), Normative Belief (NB) and Self-Efficacy (SE). From this perspective, this means that ISC would influence these three ISP compliance behavior factors. As discussed in Section 2.13.1 (Chapter 2), few studies (Dugo, 2007; Flores & Ekstedt, 2016; Parsons et al., 2015) have examined parts of these particular relationships with mixed findings. These studies also did not use a clear and consistent ISC concepts. Therefore, it is difficult to justify these findings in recognizing which concept of ISC is applicable in relation to ISP compliance behavioral factors.

Accoding to Mahfuth et al. (2017), ISC will change the behavior and attitude of employees in dealing with the information assets. The ISC's principles, activities and programs introduced and conducted will educate and improve employee's awareness, attitude, knowledge and skills in dealing with information assets (Fagade & Tryfonas, 2017). It will formulating normalized thinking and behavior modes (Tang et al., 2016) and develops knowledge, an understanding and a comprehension of precaution to advance employees' own skill levels correctly (Alhogail et al., 2015).

Furthermore, ISC eventually will promote improvement in information security practice (Alfawaz et al., 2010; Williams, 2009b) and will reduce security incidents as well as minimize information security risks that might arises (Alfawaz et al., 2010; Alhogail, 2015b; D'Arcy & Greene, 2009; Da Veiga and Eloff, 2010; Shahibi et al., 2012). As such, it is clear that ISC is crucial to be established as a strong connection with organization in shaping the way that employees feel, behave, perform, contribute, require and interact especially towards information security in an organization (Zakaria, Jarupunphol, & Gani, 2003). The establishment and cultivation of ISC is a

management's efforts and commitment designed to improve information security performance (Schlienger & Teufel, 2003b). These efforts and commitment are championed and showed by top managers and seen by all employees, as it is an indicator that top management and all employees understand and believe information security is important to the organization. Drawing from all these arguments, this study hypothesized that:

H1: ISC positively influences employee's Attitude towards compliance with ISP.

H2: ISC positively influences employee's Normative Belief about ISP compliance.

H3: ISC positively influences employee's Self-Efficacy to comply with ISP.

3.5.3 The Role of Attitude, Normative Belief and Self-Efficacy towards ISP Compliance Intention

As this study is about developing ISC model to predict particular employees' behavior towards compliance intention (INT), a well-established Theory of Planned Behavior (TPB) by Ajzen (2005) is adopted as fundamental behavior theory in forming nomological core of the research model. This theory is the most common applied and proved to be the most significant and dominant theory in explaining employees' ISP compliance behavior in the literature. It claims behavior of a person is determined by his or her intention. According to Hu et al. (2012), although the goal of TPB is to understand and predict individual behavior, measuring the actual behavior (ACT) has not been an easy task for scholars, especially those studying in organizational settings. Therefore, considering strong correlation between intentions and actual behavior (Ajzen, 2005), when facing practical difficulties to measure actual behavior, researchers often choose to investigate behavioral intentions as Dependent Variable (DV) (e.g., Bulgurcu et al., 2010a; Gefen, Karahanna, & Straub, 2003; Herath & Rao, 2009a, 2009b; Pavlou & Fygenson, 2006; Siponen & Vance, 2010). As such, this current research also uses INT as the main DV.

In addition, as discussed in Section 2.11.6 (Chapter 2), the use of INT is more significant and practical than ACT when utilizing TPB in a research model. Table 2.5 in

Section 2.11.4 (Chapter 2) also shows that most of the recent studies that adopted TPB in the research model also used INT as dependent variable instead of ACT. Moreover, since data of this study was collected by self-report, it is not suitable to use ACT because it may cause Common Method Bias. According to Workman et al. (2008), self-reports are not sufficient predictors of employees' actual behavior because employees' self-reported perceptions of security behavior are not necessarily in line with their actual behavior.

In TPB, intention is assumed to capture motivational factors that influence individual's behavior. There are three constructs that determine intention, which are Attitude towards the behavior (ATT), Normative Belief (NB), and Self-Efficacy (SE). ATT refers to a person's judgment as to whether it is good or bad to perform a behavior of interest. NB reflects the person's perceptions of whether the behavior is accepted and encouraged by his or her social circles consisting of people who are important to him or her. In an organizational setting, when behavior of interest is associated with organizational policies and practices, the person's relevant social circle of important people is made up of his or her colleagues, subordinates, and superiors. SE is the perceived ease or difficulty of performing a behavior and personal sense of having the skills and resources to perform it (Ajzen, 2005).

Specifically, in this study, attitude towards ISP compliance refers to the degree to which an individual thinks it is personally favorable or unfavorable to comply with the ISP (Fishbein & Ajzen, 1975; Bulgurcu et al., 2010a). Normative beliefs are defined as "an employee's perceived social pressure about compliance with the requirements of the ISP caused by behavioral expectations of such important referents as executives, colleagues, and managers" (Ajzen, 1991; Bulgurcu et al., 2010a). Finally, Self-Efficacy can be defined as "an employee's judgment of personal skills, knowledge or competency about fulfilling the requirements of the ISP" (Bandura, 1977; Bulgurcu et al., 2010a).

Most studies in the literature proved that the three constructs of Attitude, Normative Belief and Self-Efficacy have significant influence toward employees ISP compliance intention. Recent review in Section 2.11.4 (Chapter 2) also supports this fact. All ISP compliance studies employing TPB found that these three constructs were found significant in influencing employees' ISP compliance intention (Al-Omari et al.,

2013; Bulgurcu et al., 2010a; Hu et al., 2012b; Humaidi & Balakrishnan, 2013; Ifinedo, 2012, 2014b; Kim et al., 2014; Kranz & Haeussinger, 2014; Sommestad, Karlzén, et al., 2014). In other words, the main constructs of TPB are the most consistent factors in providing significant impact towards intention to comply in the literature compared to other behavioral theories such as PMT and GDT. Adapting the propositions of TPB to the context of organizational information security particukarly in Malaysian public universities, this research hypothesized that:

H4: Attitude towards ISP compliance positively influences employee's intention to comply with ISP.

H5: Normative Beliefs about ISP compliance positively influence employee's intention to comply with ISP.

H6: Self-Efficacy to comply with ISP positively influences employee's intention to comply with ISP.

3.5.4 The Role of Attitude, Normative Belief and Self-Efficacy in Mediating the Relationship between ISC and Intention to Comply

D'Arcy and Greene (2014) found that ISC has significant effect towards employees' intention to comply with ISP (INT). However, it is unclear whether ISC directly influences INT or the effect of ISC is mediated by other organizational or individual level factors. Specifically, from theoretical perspective of Theory of Planned Behavior (TPB), this relationship needs more explanation. It is because according to this well-known behavioral theory, a person's intention towards a particular behavior depends on three behavioral factors of Attitude (ATT), Normative Belief (NB) and Self-Efficacy (SE). Strong empirical findings further proved that these three main constructs of TPB are the strongest predictors for INT. Considering these facts, there is a possibility that these three behavioral constructs intervene the relationship between ISC and INT.

Apart from D'Arcy and Greene (2014), other studies in information security behavior literature also suggested that ATT, NB and SE play significant roles in mediating the relationship between independent variable and dependent variable. Specifically, Hu et al. (2012) found that these three factors play significant roles in

mediating the relationship between OC and INT. Since ISC is a subculture of OC, these findings suggest that the three main constructs of TPB would also mediate the relationship between ISC and INT.

More recently, Flores and Ekstedt (2016) found that ATT and NB have mediated the relationship between ISC and employee's intention towards resisting to social engineering. However this study by Flores and Ekstedt (2016) is not the same as this research in several aspects. First, dependent variable used in their study was "intention to resist social engineering", which is different from ISP compliance intention. Second, ISC concept used in their study was not based on specific dimensions that could represent the aspects in establishing a positive ISC. Third, their study did not examine the relationship based on complete view of TPB by excluding Self-Efficacy construct in the research model. Therefore, it remains unclear whether these three behavioral factors mediate the relationship between ISC and INT from a complete TPB's perspective. These examinations provides better understanding on the relationships between ISC and INT. It determines whether the relationship between ISC and ISP compliance behavior could be explained by these three significant behavioral factors. Apart from complementing the relationship theorized by TPB that intention is influenced by ATT, NB and SE, the examination justifies the adoption of TPB in the model and suggests the importance of these behavioral factors to be promoted in ensuring security behavior in the organization including Malaysian public universities. Based on these arguments, it is hypothesized that:

H7. The relationship between ISC and intention to comply is mediated by Attitude towards ISP compliance intention.

H8. The relationship between ISC and intention to comply is mediated by Normative Belief towards ISP compliance intention.

H9. The relationship between ISC and intention to comply is mediated by Self-Efficacy towards ISP compliance intention.

Summary of hypotheses for H1, H2, H3, H4, H5 and H6 is illustrated as in Research Model in Figure 3.9. Meanwhile, hypotheses for mediation relationship of H7, H8 and H9 are depicted in Figure 3.10, Figure 3.11 and Figure 3.12 respectively.

With this research model, Research Question 2 is answered and Research Objective 2 is achieved.

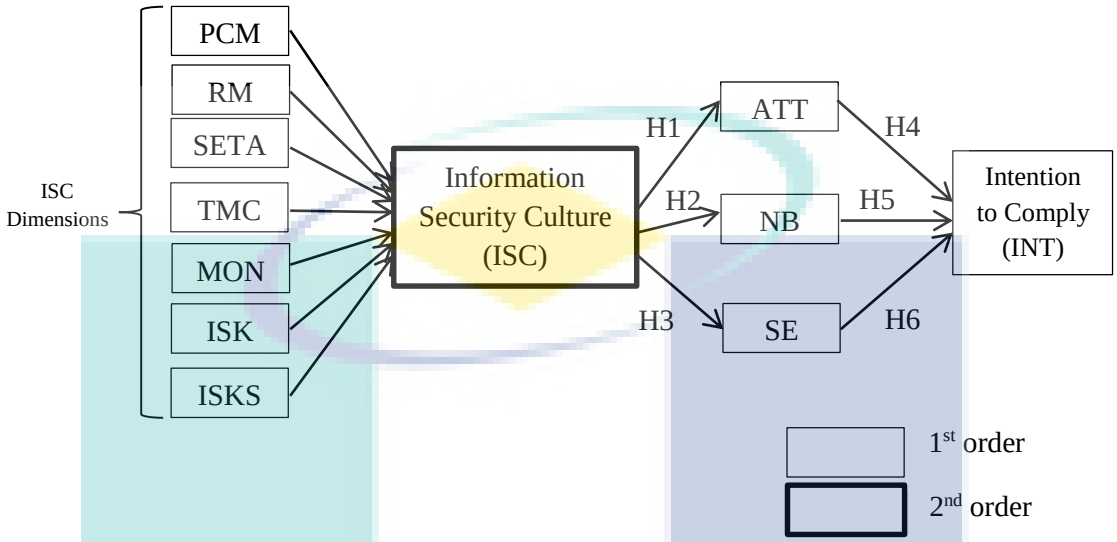
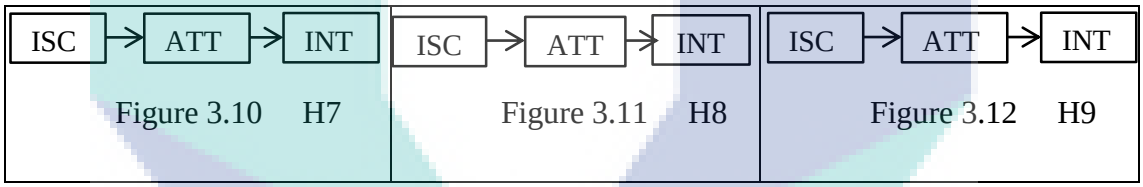


Figure 3.9 Research Model



3.6 Chapter Summary

This chapter discusses theoretical background, conceptual framework and hypotheses developed for this study. The conceptual framework was developed by integrating new concept of ISC based on formulated dimensions with the most significant theoretical framework in area of ISP compliance study, which is TPB. The ISC dimensions representing holistic concept of ISC were developed by adopting two widely accepted concepts in ISC-related studies, which are Organizational Culture by Schein (1999) and level-approach of ISC framework by Van Niekerk and Von Solms (2006) in order to justify the development process. A set of hypotheses was proposed to be investigated in this study. A research model was developed to summarize all hypotheses of relationships to be examined. Next chapter discusses the methodology employed to achieve research objectives in this research.

CHAPTER 4

METHODOLOGY

4.1 Introduction

Previous chapter has identified theoretical background of this research and subsequently developed the research model. The proposed research model was designed to examine the relationships of seven dimensions in contributing to ISC concept as well as to examine the relationships between ISC and employees' ISP compliance behavior. This chapter describes the methodology employed to answer the research questions and to achieve the objectives set forth in Chapter 1. This chapter is divided into nine sections. Next section explains the research paradigms and design followed by the research operational framework in section three. This is followed by the explanation of every phase involved in this research. Phase one and two are explained in section four and five respectively. Section six discusses a summary of activities in phase three, which is the development of research instrument. Phase four, which are the survey and data collection process and activities are discussed in section seven. Data analysis and model validation phase is discussed in section eight. Finally, a summary of this chapter is presented in section nine.

4.2 Research Paradigm and Design

This research employed positivist paradigm. This paradigm is also known as quantitative, objectivist, scientific, experimentalist or traditionalist research paradigm (Collis & Hussey, 2003). According to Berg (2001) positivist research usually uses deductive reasoning process. It searches for relationships, and is considered accurate and reliable through validity and reliability. Based on literature analysis and theoretical frameworks, this positivist research proposes relationships and hypotheses among

variables in answering the research questions. It applies quantitative research method in examining the variables and validating the relationships hypothesized in the research model.

Quantitative studies were widely applied in both ISC (Connolly et al., 2014) and information security behavior literature (Lebek, Uffen, et al., 2014). As such, this research employed questionnaire survey as a strategy to collect data from public universities' employees in validating ISC model and testing relationships hypothesized in the research model. While the quantitative studies were widely used in both ISC and ISP compliance literature, the research method using questionnaire survey for data collection was also widely accepted in both literature of ISP compliance studies (Lebek, Uffen, et al., 2014) and ISC-related studies (Al Hogail & Mirza, 2015; Alhogail, 2015a; Martins & Eloff, 2002; Schlienger & Teufel, 2005; Veiga et al., 2007).

Specifically, according to Da Veiga et al. (2007), survey methodology could be used to study employees' opinion, attitude and behavioral patterns within the context of information security. Since this research collected and studied employees' opinion and perception on particular constructs of ISC dimensions and security behaviors, survey methodology was appropriate to be used in this research. The partial least squares approach to structural equation modeling (PLS-SEM) using Smart-PLS software was used to model and analyze the data. As for ISC concept, since it was conceptualized as a multidimensional construct formed by the new formulated dimensions, Hierarchical Component Modeling (HCM) in PLS-SEM assessment was used in this study to explore and investigate the relationships of this concept.

4.3 Research Operational Framework

Table 4.1 shows research operational framework. In general, there are five main phases. Before the main phases began in achieving the research objectives, a preliminary study was conducted with literature review for identifying, analyzing and synthesizing the findings, issues and gaps in two main literature, which are ISC and ISP compliance behavior. Review on ISC literature focuses on identifying and analyzing current ISC concepts, models and frameworks to get a clear picture on available ISC models for employees' security behavior. At the same time, the review also focuses on revealing the gaps in ISC concepts based on dimensions and their relationship with

employee's security behavior. As for review on ISP compliance behavior literature, the ultimate aim is to get a current status on key findings, themes, theories, constructs and methods used in this area of study. The outcomes of this preliminary phase are current status of findings and gaps on two literature in relation with specific Research Questions (RQs) and Research Objective (ROs) for this research. This phase also identified the theoretical frameworks to be used in the proposed conceptual framework for this research. Details on these particular reviews are discussed in Chapter 2.

4.4 Phase 1 – Formulating ISC Dimension for ISC Concept

Based on the findings and gaps as well as theoretical frameworks identified from the literature review, the first phase started with the formulation of dimensions to represent ISC concept. Organizational Culture by Schein (1999) and ISC framework by Van Niekerk and Von Solms (2006) were adopted as fundamental frameworks in formulating the dimensions. As discussed in Section 2.6.2 (Chapter 2), these two concepts are the most widely accepted concepts in conceptualized ISC. A mapping process from each level of these two concepts was performed to produce associated dimensions of ISC concept. This mapping process produced seven dimensions covering all levels in OC and ISC as well as most of the ISC key factors in literature. All processes and discussion involved in this phase are presented in Chapter 3.

4.5 Phase 2 – Proposed ISC Model for Employee's ISP Compliance Behavior

The review in Chapter 2 also focuses on identifying and analyzing the main themes used in ISP compliance behavior literature. As concluded in Section 2.11.8 (Chapter 2), it was found that TPB is the most significant behavioral theory used in this field. Its main constructs, which are Attitude, Normative Belief and Self-Efficacy, were found to be the most significant predictors of ISP compliance intention. Furthermore, TPB is the most appropriate behavioral theory to explain the influence of ISC towards employee's ISP compliance behavior compared to other competing theories such as PMT and GDT. Based on these findings, TPB is adopted to represent ISP compliance behavior of employees and to form nomological core in linking ISC concept and ISP compliance behavior. New multidimensional concept of ISC produced in phase one was integrated with TPB to produce conceptual framework of this research. Hypotheses and

research model pertaining to answering RQs for the research were then proposed. All these processes are discussed in Chapter 3.

4.6 Phase 3 – Development of Research Instrument

Since this research design applied survey method, phase three started with development of survey instrument. Most of the items were adopted and adapted from previous validated studies. The use of previous validated instruments are strongly recommended in information system research (Boudreau, Gefen, & Straub, 2001; Straub, 1989) as it increases and assures content validity and reliability of the items used for constructs in the study (Nunnally & Bernstein, 1994). Nevertheless, some new items were developed for this study. Since most respondents are Malay, two versions of the questionnaire, which were in English and Bahasa Melayu were produced. For this purpose, items in the questionnaire underwent translating process. Additionally, the items underwent localizing process whereby they were adapted to Malaysian context since most items were originally applied to non-Malaysian context. Series of pre-tests were conducted to improve and refine the instrument. Face validity test was conducted for these questionnaire using group of experts from academic and IT professional. Then, the questionnaire were pre-tested using focus group of 20 respondents to examine whether the materials were understandable, clear and appealing. The information gained from this test was used to refine the questionnaire. A pilot study using this improved version was conducted in one of Malaysian public universities to test the capability of the questionnaire before actual data collection could be performed. Details of research instrument development processes and activities are discussed in Chapter 5.

4.7 Phase 4 – Survey

This phase decides the sampling strategy and sample size used in the data collection. By using final version of research instrument produced in phase three, data was collected using selected sampling strategy and targeted sample size.

4.7.1 Sample and Population

Based on data provided by Ministry of Higher Education (MoHE) (Ministry of Higher Education, 2018), all public universities are funded by the government and they are quite similar in terms of size of the organization. As for private HEIs, they vary in

terms of funding and size. Thus, this suggests that public universities have the same type of settings; whereas, private HEIs have various settings and are made of many types of institutions. All public universities in Malaysia could be assumed as having the same organizational culture since they reside under the same ministry, implementing the same educational plan from the ministry and having the same educational philosophy. They also adopt the same ISP recommended by Malaysian Government, which is from MAMPU. Since this study is all about ISC and the literature suggests that ISC depends on type and size of the organization, this study focuses only on public universities because they are different from private unversities. The reason is the findings especially ISC model could solidly represent one type of organization, which is public university without any mixed data from private university.

The population or sampling unit of this study is any public university employee that uses the computer in his/her work. Although the population of this public university is big, convenient sampling technique was used because the homogeneity of population. The reason is public university staff in Malaysia have the same attributes in terms of job scopes and working environment. Convenience sampling is a sampling procedure to obtain people who are easily available (Zikmund, 2003). Moreover, there was no complete sampling frame available for this population. Although information about number of public university staff is available and can be requested from Higher Education Ministry, this information is based on analysis of previous years. In addition, the information is about academic staff only. In this study, both academic and non-academic staffs were included. In other words, it was difficult and nearly impossible to attain the latest and current number of academic and non-academic staff for public universities in Malaysia. Since this research objective is to generalize theory based on findings rather than generalizing the sample and considering other aspects such as sampling strategy, sampling objective and complete sampling frame; thus, non-probability sampling (Ali Memon, Ting, Ramayah, Chuah, & Cheah, 2017) with convenient sampling technique was deemed appropriate for this study.

This study employs PLS-SEM for data analysis; hence, sample number must follow recommended guideline so that the best findings could be concluded. There are several techniques employed to calculate the sample size in this research. Hair, Hult, Ringle, and Sarstedt (2014) suggested minimum sample for PLS-SEM analysis is

according to maximum number of arrowheads pointing at a particular construct occuring in the measurement model. Hair et al. (2014) also recommended to follow more elaborative recommendations such as those provided by Cohen (1992) that also takes statistical power and effect sizes into account. A software named G*power program (Faul, Erdfelder, Buchner, & Lang, 2009) was used to calculate minimum sample size. Finally, this research also used recommendations by Westland (2010) in Management Information System (MIS) research that has used SEM technique. According to this recommendation, ten cases per indicator were suggested to determine appropriate sample size.

4.7.2 Data Collection Procedures

This cross-sectional study employed convenient sampling technique in collecting data using judgemental and snowball sampling strategies. The primary data collection was conducted by sending invitation to target respondent by e-mail asking them to participate in the survey using Google Forms. This e-mail also acted as a cover letter explaining purpose of the study, the information about voluntariness, confidentiality, and anonymity. Example of e-mail sent to respondents is attached in Appendix A. Additionally, a letter of declaration as in Appendix B from FSKKP, UMP is also attached in the e-mail as evidence to ensure the e-mail is genuine.

E-mail addresses of the respondents were taken from their universities websites. These websites also provide short information regarding the respondents' profiles. Based on judgemental sampling, e-mail invitation was sent to selected respondents. Careful implementation of sending these e-mails was needed to prevent from being blocked or blacklisted by the universities' server due to suspected scam mails. To avoid privacy violation and reduce spam e-mail concern, no tracking mechanism was conducted for checking the responses. For the same reason, there is no reminder e-mail was sent. Therefore, only 20 – 30 e-mails were submitted to each respondent from the same universities and this process took about three months from 30th August until 30th November 2017. The forms were also distributed through WhatsApp Application message to selected groups and people who were recognized as employees of various Malaysian public universities employees. This message contains a link to the same survey questionnaire as used in the e-mail. All responses were administered and recorded using database system provided by Google Forms.

Table 4.1 Research Operational Framework

Phase	Main Activities	Outputs	Chapter in Thesis	Research Objectives
Preliminary Study Identifying and analyzing current findings and gaps in the relationship between ISC and ISP compliance behavior	1. Identify current findings and gaps in ISC models, concepts and frameworks based on dimensions 2. Identify and analyze theories/concepts/models and approaches used to conceptualize ISC in literature 3. Identify and analyze theories, factors and other key themes in ISP compliance behavior literature	Clear status of the gaps on the relationship between ISC and ISP compliance behavior	Chapter 2	
Phase 1 Formulating Dimensions to represent ISC concept	1. Select and justify the concepts of Organizational Culture and ISC to be used in formulating the dimensions to represent the ISC concept 2. Map the levels in Organizational Culture and ISC framework into dimensions of ISC 3. Compare and justify the formulated dimensions with ISC key factors in literature	Multidimensional ISC concept based on seven dimensions	Chapter 3	RO 1: To formulate ISC dimensions based on widely accepted concepts of Organizational Culture and Information Security Culture
Phase 2 Developing ISC model based on new formulated dimensions for ISP compliance behavior	1. Select and justify TPB as a theoretical framework to represent employee's ISP compliance behavior that links ISC and ISP compliance behavior	A model of ISC based on seven dimensions for employee's ISP compliance behavior	Chapter 3	RO 2: To develop a model of ISC based on new formulated dimensions for employee's ISP compliance behavior.

Table 4.1 continued

Phase	Main Activities	Outputs	Chapter in Thesis	Research Objectives
	2. Develop hypotheses and conceptual framework on the relationship between ISC and ISP compliance behavior 3. Develop a model of ISC based on new formulated dimensions for employee's ISP compliance behavior			
Phase 3 Development of Research Instrument	1. Adopt and adapt items from previous validated studies 2. Develop new items when necessary 3. Translate and localize items 4. Pre-test with three experts in the field of information security and three academicians 5. Focus-group pre-testing 6. Pilot study	Survey Questionnaire	Chapter 5	RO 3: To validate the formulated dimensions in representing ISC conceptual model RO 4: To validate ISC model for employee's ISP compliance behavior in Malaysian public universities RO 5: To validate the roles of Attitude, Normative Belief and Self-Efficacy in mediating the relationship between ISC and ISP compliance intention
Phase 4 Survey	1. Determine population and sample size 2. Data collection	Sample size, Data	Chapter 5	
Phase 5 Data analysis and model validation	1. Data screening 2. Data analysis 3. Hypotheses testing 4. Model validation 5. Conclusion	Validated ISC concept and model for ISP compliance behavior	Chapter 6	

Overall, 5000 e-mails were sent to targeted respondents. However, hundreds of undelivered e-mail responses were received due to several reasons such as incorrect e-mail addresses, rerouted to junk folder, un-opened by recipients (Ranchhod & Zhou 2001) and e-mails were not used anymore. This survey received 634 responses out of 5000 e-mails sent and the response rate is 12.6%. Although this rate seems to be low, low response rates are not unusual in random targeted e-mail survey (Spears & Barki, 2010). According to Guo and Yuan (2012), survey repondents usually simply deleted survey e-mail without reading or declined to respond because they do not have time. Moreover, nowadays they are more sceptical to provide information on the Internet due to increasing awareness campaigned by various parties on security and privacy of information. Since the collection was conducted using e-mail survey, this response rate is consistent with Fan and Yan (2010); Spears and Barki (2010) who found the response rate for this mode is significantly lower than other survey modes. Nevertheless, this response rate is relatively high given the problems typically encountered when collecting sensitive security-related data from organizations (Hina & Dominic, 2017; Kotulic & Clark, 2004). Since the response rate was considered high and the number of responses exceded minimum number of desired sample size, the nonresponse bias was not an issue for this study. Furthermore, study by Groves and Peytcheva (2008) also found that no overall significant correlation of response rate and nonresponse bias. Since this study did not track and remind the respondents; thus, this study could not identify non-respondents in data collection process.

4.7.3 Data Screening

Before data being analyzed, the screening process was conducted to detect any missing values and outliers. One of the advantages using on-line form in collecting data is in its setting ability whereby respondents were required to respond to each question without skipping any item. Since the items for the main constructs were set in this mode, there is no missing value for the main constructs used in the study.

4.8 Phase 5 - Data Analysis and Model Validation

In this phase, the collected data was analyzed to test the hypotheses and validate the model proposed. Details for the results, analysis and discussions on the findings are discussed in Chapter 6.

4.8.1 Data Processing and Analysis

The research model was validated using second generation statistical analysis technique called Structural Equation Modeling (SEM). This technique has recently grown popular in Information System (IS) research (Aziz & Kamaludin, 2014; Roberts & Grover, 2009) particularly in information security behavioral research (e.g. Hanus & Wu, 2016; Kim et al., 2014; Safa et al., 2015). Moreover, recent ISC model developed by Martins and Da Veiga (2015a) was also validated using SEM technique. For current study, Partial Least Squares (PLS) modeling technique was used to analyze data via the SmartPLS version 3.2.4 (Ringle, Wende, & Becker, 2015) software package.

Since this research focuses on exploratory model and theory development especially on ISC concept, PLS was considered to be more adequate for this study. In general, this research investigates and explains ISC concept based on new formulated dimensions and how this multidimensional concept influences ISP compliance behavior. Specifically, this research investigates the relationship of formulated dimensions with ISC concept. This means that ISC is conceptualized as a multidimensional higher-order construct formed by new formulated dimensions of lower-order constructs. As such, PLS-SEM is the best solution because it supports the testing of both reflective and formative relationships between higher-order constructs and their sub-constructs. Furthermore, PLS-SEM method has the ability to handle reflective and formative measurement scales (Jarvis, MacKenzie, & Podsakoff, 2003). The capability of PLS-SEM allowing multiple dependent variables in the research model to be examined simultaneously in this study was also the reason for its selection. ISP compliance behavior is represented by TPB and this theory states that Intention (INT) is determined by Attitude (ATT), Normative Belief (NB) and Self-Efficacy (SE). Therefore, three intermediate Dependent Variables (DV) and one main DV are simultanously examined in this research. In other words, this research examines the influence of ISC towards ATT, NB and SE as well as the influences of ATT, NB and SE towards INT.

In addition, PLS-SEM was used because this study is more on prediction and explanation of target constructs (Hair et al., 2014). Besides examining ISC as a multidimensional construct, this study develops an exploratory model of ISC concept that could predict ISP compliance behavior of employees in the organization. As such,

there are several constructs contain in the model including multidimensional construct of ISC, its lower-order constructs and behavioral constructs of ISP compliance behavior. Therefore, this study investigates how particular constructs of employees' ISP compliance behavior factors and intention are predicted by ISC perception of the organization. As behavior constructs are also dependent varibles (DV), it investigates how the variances in these intermediate and main DV constructs could be predicted and explained by exogenous constructs in the model. This is consistent with Sarstedt, Ringle, Smith, Reams and Hair (2014) who suggested the use of PLS-SEM if the research goal is to predict one or more key target construct(s) or to identify the most important antecedents of the target construct(s).

This research also employed Statistical Package for Social Science (SPSS) version 18.0. The software was used to screen data in terms of outliers, normality and for common method bias tests. This software was also used to compute frequencies, means and standard deviations to gain an overview of the data especially in the earlier stage of analysis.

4.8.2 Evaluation of PLS-SEM Results

Figure 4.1 illustrates summary of data analysis procedures applied in this research. Phase one started with data screening procedures to ensure they were correctly entered and free from straightlining, outliers as well as missing values. Straightlining refers to responses that have the same answers for all questions or answers that form certain patterns in a questionnaire (Hair et al., 2014). Outlier is an extreme response to a particular question, or extreme responses to all questions. Checking for outliers is important as outliers could affect the normality of data which could then distort statistical results (Hair, Black, Babin, & Anderson, 1998; Tabachnick & Fidell., 2001).

This phase also involved the examinations of Common Method Variance (CMV) and data normality. CMV is defined as "variance that is attributable to the measurement method rather than to the constructs the measure represent" (Podsakoff et al. 2003, p.289). This systematic error variance can cause common method bias and can cause bias to the estimated relationships among variables or measures (Campbell & Fiske, 1959; Jakobsen & Jensen, 2015). In this research, CMV was examined using three tests, which are Correlation Matrix (Bagozzi, Yi, & Phillips, 1991), Harman's

Single-Factor Test (Podsakoff & Organ, 1986) and Partialling Out a "Marker" Variable Podsakoff et al. (2003). Finally, univariate and multivariate normality tests for examining the data normality were conducted as the last procedure in this first phase.

Then, the second phase commenced. By following two-stage approach by (Anderson & Gerbing, 1988; Hulland, 1999), measurement model was assessed first to ensure the validity and reliability of measurements. Then, it was followed by analysis of the structural model to test research hypotheses and overall quality of the proposed model. The next sub-sections discuss the assessments and procedures in these two stages.

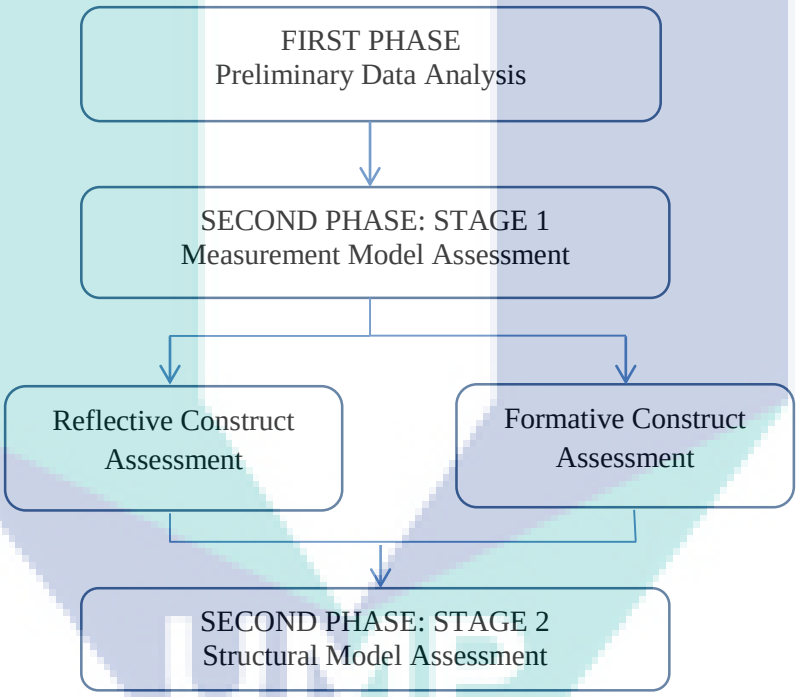


Figure 4.1 Summary of Data Analysis Procedures

4.8.2.1 Measurement Model Assessment Procedure and Criteria

Quality of the measurement model was assessed differently according to the type of construct as recommended in PLS-SEM. For reflective constructs, the quality of the measurement model was assessed by three criteria, which are composite reliability, convergent validity and discriminant validity.

Reliability of the measurement addresses the concern of how well the items for one construct correlate or move together (Straub et al., 2004). It evaluates the degree to which responses are consistent across the items (Kline, 2005). In this study, reliability was assessed by two statistics, which are Cronbach's Alpha and Composite Reliability (CR). Cronbach's Alpha is a measure of internal consistency reliability that assumes equal indicator loadings (Hair et al., 2014). Composite reliability addresses a similar concept but is considered a more rigorous reliability measure in the context of structural equation modeling (Chin, 1998; Raykov, 1998). The scores of Cronbach Alpha more than 0.70 (Bagozzi & Yi, 1988; Gefen, Straub, & Boudreau, 2000) and more than 0.80 for CR (Chin, 2010) respectively indicate the measurements have acceptable reliability in measuring the constructs.

The second criterion of measurement model assessment is convergent validity. It is the extent to which an item of measurement correlates positively with alternative items of the same construct. The assessment was conducted by evaluating the indicators' factor loading and Average Variance Extracted (AVE). In this assessment, all factor loadings should exceed 0.708 and AVE for each construct should exceed 0.50 (Hair et al., 2014).

The last criterion assessed in measurement model assessment is discriminant validity. It refers to the extent to which a construct distinctly differentiates from others. At the indicator level, discriminant validity was assessed by analyzing item cross-loadings. In this assessment, the difference of indicator's outer loading on the associated construct should be greater than 0.10 (Hair, Hult, Ringle, & Sarstedt, 2013) on all of its loadings on other constructs (i.e., the cross loadings) (Hair, Ringle, & Sarstedt, 2011). At the construct level, discriminant validity was examined by comparing square root of each construct's AVE against its correlation with other constructs (Fornell & Larcker, 1981). Square root of each AVE must be greater than the correlations between constructs, indicating that more variance is shared between the construct and its indicators than with other constructs. Instead of using these two tests, additional test using HTMT approach as recommended by Henseler, Ringle and Sarstedt (2015) was also employed in this study. According to this criterion, if HTMT value is below 0.90, discriminant validity is established between two reflective constructs.

4.8.2.2 Measurement of Multidimensional Second-Order Construct

One of the main objectives of this research is to validate ISC concept as a second-order construct formed by formulated dimensions. This validation is to examine the relevance and significance of these dimensions in contributing to the underlying concept of ISC. This conceptualization and operationalization also enable proper way to investigate effects of a construct that could be measured by several related constructs. Basically, two approaches could be used to assess second-order construct, which are repeated indicator approach and two-stages approach (Hair et al., 2014). This study employed repeated indicator approach with Mode A and path weighting scheme to model second-order factors in PLS analysis. This approach produces more precise parameter estimates and more reliable higher-order construct score for reflective-formative hierarchical constructs (Becker et al., 2012; Wilson & Henseler, 2007). It works best in the case of all first-order constructs have the same or comparable number of items (Hair, Sarsted, Ringle, & Guderga, 2018). While path weighting scheme is the recommended structural model by Hair et al. (2014), the main benefit of repeated indicator approach over two stages is the ability to estimate all the latent variables simultaneously instead of estimating Higher-order Construct (HOC) and Lower-order Constructs (LOC) separately (Tehseen & Gadar, 2017). Therefore, this approach prevents interpretational confounding by taking the whole nomological network into consideration (Becker et al., 2012).

According to Hair et al. (2018), Mode A corresponds to correlation weights derived from bivariate correlations between each indicator and the construct. Mode B corresponds to regression weights, the standard in ordinary least squares regression analysis. Formative type models are commonly estimated by using Mode A for repeated indicators, in the case of first-order constructs are reflective (Chin, 2010; Hair et al., 2018; Ringle, Sarstedt, & Straub, 2012). This approach was also recently proven in validating formative second-order construct with reflective first-order constructs in other fields such as business and marketing (Duarte & Amaro, 2018; Tehseen & Gadar, 2017). Furthermore, since ISC construct is exogenous in the research model, the repeated indicator approach is appropriate as two-stages approach is appropriate when the second-order construct is endogenous (Duarte & Amaro, 2018). Therefore, this approach is suitable since the primary objective of this study is to investigate the

relationships of the formulated dimensions towards ISC concept as well as to investigate how this ISC concept influences employee's ISP compliance behavior. In this approach, a higher-order latent variable was constructed by specifying a latent variable that represents all manifested variables of the underlying lower-order latent variables (Lohmöller, 1989; Wold, 1982; Wold & Noonan, 1983).

In assessing ISC as a formative second-order construct, two main criteria were used, which are significant and relevant of indicator weights as well as indicator collinearity (Hair et al., 2011). For this purpose, a bootstrapping procedure was employed to assess whether a formative indicator significantly contributed to its corresponding construct by assessing the outer weight significance and relevance. The weights of the formulated dimensions towards the second-order construct of ISC were assessed to examine whether each subdimension significantly contributed to the underlying overall factor by using guidelines recommended by Lohmöller (1989); Becker et al. (2012); Wright, Campbell, Thatcher, and Roberts (2012); and Wetzels, Odekerken-Schröder, and Oppen (2009).

According to Becker et al. (2012), these weights are important as they represent actionable drivers of higher-order construct, which is in this case is ISC. The significance of each dimension was assessed to understand the relative association of each dimension to multidimensional construct of ISC (Wright, Campbell, Thatcher, & Roberts, 2012). Finally, confidence intervals as well as p-values for formative indicators were assessed to provide additional evidence regarding the significance of weights.

Since the relationship of ISC with the first-order constructs is formative, the reliability was assessed as the same way as formative construct (Hair et al., 2014). Formative scales are not subjected to the same validity and reliability criteria as reflective constructs (Diamantopoulos & Winklhofer 2001, Jarvis et al. 2003). The reliability of formative constructs was perfomed by assessing the collinearity of indicators. Variance Inflation Factors (VIF) value for each construct should not be above the value of 5 to assure collinearity of the formative constructs does not reach the critical levels.

4.8.2.3 Structural Model Assessment Procedure and Criteria

According to Hair et al. (2014), assessment of the structural model results determine how well empirical data support the theory or concept in order to decide if the theory or concept has been empirically confirmed. In structural model assessment for this study, model's predictive capabilities and the relationships between the constructs were examined by estimating path coefficients and R^2 value. Figure 4.2 shows a systematic approach to the assessment of structural model results. As recommended by Hair et al. (2014), structural model assessment should started by checking the structural model for collinearity issues. VIF values below than 5 indicate that no issue of collinearity among the constructs occurs in the structural model.

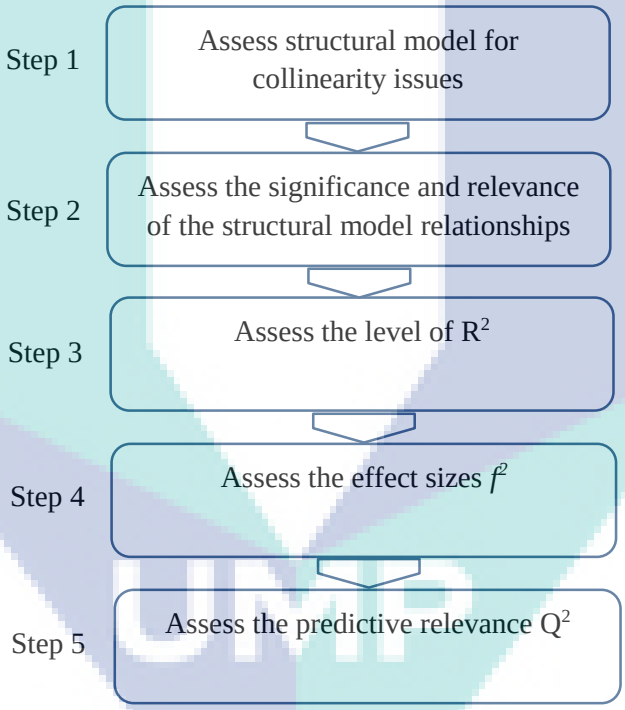


Figure 4.2 Structural Model Assessment Procedure
Source: Hair et al. (2014)

Then, in the second step, the significance and relevance of the structural model relationships were assessed. In this study, path coefficients with a 5% or less probability of error were considered as significant. Since there are recommendations that suggest to report *t*-value in determining the significance of path coefficients, a bootstrapping procedure was performed to calculate this *t*-value. For this study, the *t*-value of 1.65

(one-tailed) and above was considered as significant for relationships hypothesized in the model. According to Hair, Ringle, and Sarstedt (2011), critical *t*-values for one-tailed test are 1.65 ($p<0.05$), and 2.33 ($p<0.01$).

The third step was to assess the level of R^2. Coefficient of determination (R^2 value) is a measure of the model's predictive accuracy and was calculated as squared correlation between a specific endogenous construct's actual and predicted values (Hair et al., 2014). R^2 value indicates the amount of variance in dependent variable explained by all independent variables linked to it. In general, R^2 values of 0.75, 0.50, or 0.25 for the endogenous constructs can be described as respectively substantial, moderate, and weak (Hair et al., 2014). However, in behavior research especially consumer behavior, R^2 of 0.2 is considered as high (Hair et al., 2014). Furthermore, according to Cohen (1988), R^2 values of 0.26, 0.13 and 0.02 are considered as substantial, moderate and weak respectively. Therefore, R^2 values for endogenous constructs for this study were analyzed accordingly based on research context and complexity of the model.

Then, the fourth step was to assess the Effect Size (f^2). This assessment allows assessing an exogenous construct's contribution to an endogenous latent variable's R^2. The f^2 values of 0.02, 0.15, and 0.35 indicate an exogenous construct's small, medium, or large effect, respectively, on an endogenous construct (Cohen, 1988). In this study, this examination assessed the individual impact of ISC towards ATT, NB and SE as well as ATT, NB and SE towards INT to see whether these particular exogenous constructs had small, medium or large effects on the respective endogenous constructs.

The last step in structural model assessment was to assess the predictive relevance, Q^2 (Geisser, 1974; Stone, 1974). According to Hair et al., (2014), besides assessing the model's predictive accuracy, model's predictive relevance should also be assessed to accurately predict data points of indicators in reflective measurement models of endogenous constructs. Predictive relevance, Q^2 (Geisser, 1974; Stone, 1974) of the model is assessed by using blindfolding procedures (Chin, 1998; Henseler et al., 2009; Tenenhaus et al., 2005). Q^2 value that is larger than zero for a certain reflective endogenous latent variable indicates the path model's predictive relevance for this particular construct. In this study, it assessed the predictive relevance of path model for constructs of ATT, NB, SE and INT. According to Hair et al. (2014), Q^2 values larger

than zero for a certain reflective endogenous latent variable indicate the path model's predictive relevance for these particular constructs.

4.8.2.4 Mediation Analysis

This research also examines the effects of three behavioral factors of ATT, NB and SE as mediator in the relationship between ISC and INT. This examination is crucial because it indicates the importance of these three behavioral factors to be promoted as an effort to increase security behavior in the organization. The examination also important to better understand the causal relationship and reveal intervening construct(s) that influence this relationship. Mediating analysis involves establishing theoretical indirect relationship between constructs to determine the degree to which indirect effects through the mediating variables modify the hypothesised direct paths. By using recommendation by Memon et al., (2018), this study used transmittal approach (Rungtusanatham, Miller, & Boyer, 2014) in hypothesing the mediation. This approach requires a single hypothesis stating that mediator (M) mediates the relationship between independent variable (X) and outcome variable (Y) without delving into hypotheses relating X to M and M to Y.

According to Memon et al. (2018), there is no requirement to test direct relationship between X and Y in mediation analysis. The relationship between X and Y 'needs not be considered when determining whether M mediates the effect of X on Y because that path is not part of mediated effect' (Aguinis et al., 2017, p. 12). In this study, the mediation analysis was conducted by following the approaches by Preacher and Hayes (2004) and Zhao et al. (2010). The mediation test was conducted without the precondition that the relation between X and Y should be significant (Aguinis, Edwards, & Bradley, 2017). A bootstrapping procedure with 5000 sub-samples was conducted for each mediating construct hypothesized in this study. A mediation exists when the indirect effect is supported, regardless of the presence or absence of a direct effect (Aguinis et al., 2017). In this research, an indirect effect with t-value > 1.56 (two-tailed) and p-value < 0.05 is considered significant (Preacher & Hayes, 2008; Zhao, Lynch, & Chen, 2010). In addition, Confidence Intervals (CI) for the indirect effect relationship were examined as additional assessment to confirm the mediation effect. CI value of Lower Level (LL) and Upper Level (UL) that does not straddle a zero in between is an indication of the presence of mediation effect (Memon et al., 2018).

4.9 Chapter Summary

This chapter discusses and justifies the need to employ a quantitative research methodology in gathering answers to the research questions and testing the hypotheses in the model. The chapter has detailed the methods used in this research, including the research design and processes, sampling and population, data collection procedures as well as data analysis procedures. Next chapter discusses the development of research instruments to collect data for model validation.

CHAPTER 5

RESEARCH INSTRUMENT DEVELOPMENT

5.1 Introduction

This chapter discusses the development of research instrument for measuring the constructs in the research model. It consists of nine sections. The next section discusses the process of items development followed by the discussion of Likert Scales in section three. The process of translating the items including items localizing is discussed in section four. Section five discusses regarding demographic variables and section six elaborates control variables. Then, the section continues with discussions on pre-tests and pilot test in section seven and section eight respectively. This chapter is concluded with a short summary in section nine.

5.2 Questionnaire Items

Research model developed in previous chapter consists of eleven first-order latent constructs and one second-order construct. All first-order constructs are reflective and measured directly by collecting data from the respondents using the questionnaire survey items. As for the second-order construct, which is ISC, it is measured and examined by using its first-order constructs' items of PCM, RM, SETA, TMC, MON, ISK and ISKS. As discussed in Section 3.5 (Chapter 3), these seven constructs represent seven dimensions that form the ISC construct.

Table 5.1 shows operational definition of each construct with its original items and sources used in this research. The following sub-sections provide overview of the items used to measure each construct in this research.

Table 5.1 Operational Definition, Items and Sources of Constructs

Construct	Operational Definition	Item Text	Source
PCM	Employee's awareness regarding ISP in the organization	PCM1: My organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use.	D'Arcy et al. (2009) Hovav and D'Arcy (2012), Chen et al. (2015)
		PCM2: My organization has established rules of behavior for use of computer resources.	
		PCM3: My organization has specific guidelines that govern what employees are allowed to do with their computers.	D'Arcy et al. (2009), Chen et al. (2015)
		*PCM4: My organization has specific guidelines that describe the acceptable use of e-mail	D'Arcy et al. (2009), Hovav and D'Arcy (2012)
RM	Employee's perception of risk analysis and assessment and whether they see it as a necessary process	RM1: Threats to information assets are controlled adequately in my organizations	Da Veiga (2008)
		RM2: I believe the risk management processes are adequate to identify the risks that could negatively impact on the confidentiality, integrity and availability of our information assets	
		RM3: It is important to understand the threats and vulnerabilities to information assets in my work environment	
		*RM4: I believe that my organization has appropriate plans for risk management.	Ismail et al. (2010)
SETA	Employee's perception regarding organizational security training activities that are related to security education, security training, and awareness-raising programs	SETA1: In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	D'Arcy et al. (2009), Hovav and D'Arcy (2012), Chen et al. (2015)
		SETA2: In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.	
		SETA3: My organization educates employees on their computer security responsibilities	
		SETA4: My organization provides training to help employees improve their awareness of computer and information security issues.	D'Arcy et al. (2009), Hovav and D'Arcy (2012)

Table 5.1 continued

Construct	Operational Definition	Item Text	Source
TMC	Top management's involvement in the organization's information security related issues from the perspective of employees	TMC1: I believed senior managers of our company have articulated a clear vision about information security.	Hu, Dinev, Hart, and Cooke (2012)
		TMC2: I believed senior managers of our company have formulated a clear strategy for achieving a high degree of information security.	
		TMC3: I believed senior managers of our company have established clear goals and objectives for achieving a high degree of information security.	
		*TMC4: Top management considers information security an important organizational priority.	Knapp et al. (2006)
MON	Employee's perception regarding organizational tracking computing activities and performing security audits	MON1: I believe that my organization conducts periodic audits to detect the use of unauthorized software on its computers.	D'Arcy et al. (2009), Hovav and D'Arcy (2012), Chen et al. (2015)
		MON2: I believe that employee computing activities are monitored by my organization	D'Arcy et al. (2009), Chen et al. (2015); ; D'Arcy & Greene (2014)
		MON3: I believe that my organization reviews logs of employees' computing activities on a regular basis.	D'Arcy et al. (2009), Hovav and D'Arcy (2012), Chen et al. (2015), D'Arcy and Greene (2014)
		*MON4: I believe that my organization monitors any modification or altering of computerized data by employees.	
ISK	Employee's perception regarding knowledge of information security posed by the organization	ISK1: There is adequate information security specialist/coordinator/person-in-charge throughout my organization to ensure the implementation of information security controls	Adapted from Da Veiga (2008)
		ISK2: I believe that information security controls implemented in my organization are in line with appropriate practice guidelines to secure information assets.	Adapted from Da Veiga (2008)
		ISK3: I believe my organization has used adequate security knowledge in implementing information security programs and campaigns.	Self-definition by referring to Van Niekerk and Von Solms (2006, 2010); Zakaria (2006)

Table 5.1 continued

Construct	Operational Definition	Item Text	Source
		ISK4: Information security programs organized by the organization have helped me improve my information security knowledge	
		ISK5: Information security programs organized by the organization have helped help me improving my security skills	
ISKS	Employee's perception regarding sharing information security knowledge in the organization and whether they see it as a necessary activities	ISKS1: I frequently share my information security knowledge in my working place in order to decrease information security risk.	Sohrabi Safa et al. (2016)
		ISKS2: I participate in information security knowledge sharing in order to keep myself up-to-date.	
		ISKS3: I think information security knowledge sharing helps me to understand the usefulness of information security policies in my organization.	
		ISKS4: I think information security knowledge sharing is an effective approach to mitigate the risk of information security breaches.	
		ISKS5: I think information security knowledge sharing is a valuable practice in organizations.	
ATT	The degree to which an individual thinks it is personally favorable or unfavorable to comply with the ISP	ATT1: To me, complying with the requirements of the ISP is important	Adapted from Ajzen (1991), Bulgurcu et al. (2010a)
		ATT2: To me, complying with the requirements of the ISP is useful	
		ATT3: Following the organization's ISSP is a necessity	Ifinedo (2014a)
		ATT4: Following the organization's ISSP is beneficial	

Table 5.1 continued

Construct	Operational Definition	Item Text	Source
NB	Employee's perception towards social pressure on complying with the requirements of the ISP caused by behavioral expectations of such important referents as executives, colleagues, and managers	NB1: My managers think that I should comply with the requirements of the ISP	Ajzen (1991); Bulgurcu et al. (2010a); Kranz and Haeussinger (2014)
		NB2: My executives think that I should comply with the requirements of the ISP	
		NB3: My colleagues think that I should comply with the requirements of the ISP	
SE	Employee's judgment on personal skills, knowledge, or competency about fulfilling the requirements of the ISP	SE1: I have the necessary skills to fulfill the requirements of the ISP	Bulgurcu et al. (2010a)
		SE2: I have the necessary knowledge to fulfill the requirements of the ISP	
		SE3: I have the necessary competencies to fulfill the requirements of the ISP	
INT	Employee's intention to comply with ISP	INT1: It is my intention to continue to comply with the organization's ISSP	Ifinedo (2012), Herath and Rao (2009a, b)
		INT2: I am certain that I will follow organizational security policies.	
		INT3: I am likely to follow organizational security policies in the future	
		INT4: I would follow the organization's security policy whenever possible	

*Added item after pre-tests (see Section 5.7)

5.2.1 Procedural Countermeasure (PCM)

As discussed in Section 3.3.1 (Chapter 3), this dimension represents information security artifacts in the organization in form of procedural guidelines or commonly called ISP. To operationalize this dimension, PCM construct measures employee's awareness regarding ISP in the organization. Four original items from D'Arcy et al. (2009) measuring ISP awareness were directly adopted to measure this reflective construct. As shown in Table 5.1, three of these items were also used to measure employee's awareness of security policy in recent studies by Hovav and D'Arcy (2012) and Chen et al. (2015).

5.2.2 Risk Management (RM)

Similar to PCM, this dimension represents information security artifacts in the organization but in form of technical countermeasures to deal with risk analysis and risk assessment. To operationalize this dimension, RM construct measures employee's perception of risk analysis and assessment, and determine if they see it as a necessary process. As shown in Table 5.1, three items of RM1, RM2 and RM3 that measure risk management's variable in Da Veiga (2008) were directly adopted for this construct. Additionally, one item, which is RM4 that measures the aspect of risk management plan in Ismail et al. (2010) was adapted to increase content validity for this construct.

5.2.3 Security Education, Training and Awareness (SETA)

As discussed in Section 3.3.2 (Chapter 3), this dimension represents information security program that espoused in the organization. It is a program that promotes the requirements, guidelines and values established in an organizational ISP. To operationalize this dimension, SETA construct measures employee's perception regarding organizational security training activities that are related to security education, security training, and awareness-raising programs. Four items of SETA1, SETA2, SETA3 and SETA4 were directly adopted from D'Arcy et al. (2009); Hovav and D'Arcy (2012). Three of these items also were used in Chen et al. (2015) to measure SETA construct in their study.

5.2.4 Top Management Commitment (TMC)

In this research, operational definition for TMC construct is top management's involvement in organization's information security related issues from employees' perspective. Similar to the construct of Perceived Top Management Participation in Hu, Dinev, Hart, and Cooke (2012), three items of TMC1, TMC2 AND TMC3 were directly adopted to measure TMC in this research. Additionally, TMC4 was adopted from Knapp et al. (2006) to cover more domain of definition for this reflective construct.

5.2.5 Monitoring (MON)

As shown in Table 5.1, operational definition for this construct is employee's perception regarding organizational tracking computing activities and performing security audits. This construct operationalizes MON dimension of ISC concept concerning employees' belief on their computing activities being monitored by their organization. Four items, which are MON1, MON2, MON3 and MON4 were directly adopted from D'Arcy et al. (2009). All these items were also employed in recent study by Chen et al. (2015) to measure security monitoring in their study. Moreover, most of these items were also used by Hovav and D'Arcy (2012) and D'Arcy and Greene (2014) in measuring the same construct in their study.

5.2.6 Information Security Knowledge (ISK)

One of unique contributions of this research is the conceptualization and operationalization Information Security Knowledge (ISK) construct in ISC and ISP compliance behavior literature. As mentioned in Table 5.1, ISK refers to employee's perception regarding knowledge of information security posed by the organization. This construct measures information security knowledge throughout an organization in improving knowledge and skill of the employees.

The measurement items for ISK construct were developed based on guidelines recommended from the literature. The factors outlined and suggested by Mackenzie, Podsakoff, and Podsakoff (2011) in conceptualizing constructs were applied for this construct. Specifically, Mackenzie et al. (2011) suggested to utilize various sources for developing the items including reviews of the literature, deduction from theoretical definition of the construct, previous theoretical and empirical research of the construct,

suggestions from experts in the field, interviews or focus group discussions with representatives of the population(s) to which the focal construct is expected to generalize, and an examination of other measures for the construct that already exist.

The development of items for this construct was based on literature analysis of this construct particularly in Van Niekerk and Von Solms (2005, 2006, 2010); Da Veiga (2008); Zakaria (2006); and Flores, Antonsen, and Ekstedt (2014), which is consistent with its dimension as discussed in Section 3.3.4 (Chapter 3). Additionally, when possible, the measurement items of the constructs were developed based on existing scales in extent literature that have been proven reliable. As a result, two items from Da Veiga (2008) were adopted since these items fit the definition and domain of the construct. These two particular items, which are ISK1 and ISK2 reflect information security knowledge in providing adequate knowledge to level one, two and three in ISC framework (Van Niekerk & Von Solms, 2006). In other words, these two items operationalize this construct in terms of how the information security knowledge provides adequate and appropriate knowledge to dimensions of PCM, RM, SETA, TMC and MON.

The first item, ISK1 measures the perception of employees towards the appropriateness of expert or person-in-charge of information security matters in the organization. This is consistent with Flores et al. (2014) that information security knowledge could be manifested through information security specialists hired to perform activities that increase information security knowledge, or having dedicated units within the organization that are responsible for those activities. This person-in-charge or unit or department represents information security knowledge posed by the organization as this unit provides adequate knowledge towards the dimensions of PCM, RM, SETA, TMC and MON. This unit is responsible for implementing those dimensions and making sure they are effective. Then, the second item, ISK2 measures an employee's perception pertaining to information security knowledge posed by organization on the ability to implement appropriate information security controls. These controls include all the countermeasures and requirements implemented in PCM, RM, TMC and MON.

Another three items were developed in this study to maximize ISK construct measurement as this construct reflects four aspects of knowledge of information

security, which are ISP, information security controls, information security programs and employees in the organization. Whilst, ISK1 and ISK2 have covered two aspects of ISP and information security controls, ISK3 measures employees' perception on information knowledge adequacy posed by the organization in providing appropriate information security programs to the employees. Then, consistent with Zakaria (2006) that adequate knowledge of information security posed by an organization ensures employees behave and practice securely when dealing with information assets, ISK4 and ISK5 measure the employees' perceptions on information security programs towards improving their information security knowledge and skills.

5.2.7 Information Security Knowledge Sharing (ISKS)

Consistent with Zakaria (2007) and Hassan et al. (2013) in Section 3.3.4 (Chapter 3) that it is essential to share information security knowledge so that all the employees attain adequate knowledge to safely deal with information security assets. Thus, operational definition for this construct is an employee's perception with regard sharing information security knowledge in the organization and whether they see it as a necessary activity. Five items measuring information security knowledge sharing in Safa et al. (2016) were directly adopted to measure ISKS construct in this research.

5.2.8 Attitude (ATT)

Consistent with Attitude construct in ISP compliance behavior literature, operational definition of ATT construct is the degree to which an individual thinks it is personally favorable or unfavorable to comply with ISP. Two items that measuring attitude towards ISP compliance in Ifinedo (2014a) were adopted as ATT1 and ATT2. Another two items, ATT3 and ATT4 are adapted from Bulgurcu et al. (2010a), which were originally taken from Ajzen (1991).

5.2.9 Normative Belief (NB)

As shown in Table 5.1, operational definition for this construct is an employee's perception about social pressure to comply with requirements of ISP caused by behavioral expectations of such important referents as executives, colleagues, and managers. Since this definition was taken directly from Bulgurcu et al. (2010), which

was originally based on TPB (Ajzen, 1991), all three items from Bulgurcu et al. (2010a) were adopted to measure NB in this research.

5.2.10 Self-Efficacy (SE)

Similar to ATT and NB, this construct was originally from TPB and its operational definition is taken directly from Bulgurcu et al. (2010a). Therefore, three items of SE from Bulgurcu et al. (2010a) were adopted to measure SE in this research.

5.2.11 Intention to Comply with ISP (INT)

As shown in Table 5.1, operational definition for this construct is an employee's intention to comply with ISP. All four items used in this research was adopted from Ifinedo (2012), who studied employee's intention to comply with ISP using TPB. All these four items are originally from Herath and Rao (2009a, b).

5.3 Likert Scales

In this research, initially, all constructs were operationalized using Likert scale to provide more accurate view of employees' attitudes and perceptions (Järvinen, 2000). Likert scale ranging from (1) strongly disagree to (7) strongly agree were applied to all constructs' items except for Attitude and Self-Efficacy. Specifically, the scale for Attitude and Self-Efficacy follows the measurement by Ajzen (1991); Bulgurcu et al. (2010a); Kranz and Haeussinger (2014). Likert scale for Attitude construct ranges from (1) extremely (necessary, beneficial, important, useful) to (7) extremely (unnecessary, unbeneficial, unimportant, useless). As for Self-Efficacy, the Likert scale ranges from (1) almost always to (7) almost never. The usage of multiple scales in a survey instrument is one of the techniques in eliminating common scale properties which reduce common method bias for this study (Podsakoff, Mackenzie, & Podsakoff, 2012).

5.4 Translation of Item

The respondents for this study are Malaysian Public Universities' employees at all levels. Most employees particularly the supporting staff are Malaysian and some of them are very comfortable using Bahasa Malaysia instead of English. Since most of the questionnaire items were adopted from previous validated studies that using English

language, the questionnaire needed to be translated in the attempt to minimize any possible variance due to cultural and linguistic differences (Kim & Han., 2004).

In this study, back-translation technique was employed to translate the items from English to Malay language. Back-translation is highly recommended by scholars and the most widely used in cross-cultural research (Brislin, 1970; Champman & Carter, 1979; Werner & Campbell, 1970; Yu, Lee, & Woo, 2004). In this process, initially, two bilingual translators competent in both English and Malay Language were involved. The first translator translated from the source language (English) into a target language (Malay Language). Another translator who was not familiar with the measurements used in the questionnaire served as the back translator. The Malay Language version was then translated back into the English version.

Once completed, the Malay Language version was reviewed by three Information Technology (IT) professionals in Malaysia. These IT professionals were asked to mark the items, words, or phrases that sounded strange or were not commonly used in their field. They also asked to comment and suggest the most suitable items, words or phrases. The two previous bilingual translators were invited to examine and discuss the comments made by IT professionals and selected the most linguistically appropriate translated sentences. The translators also evaluated cultural appropriateness of the instrument. At this stage, the decentering process was employed. Decentering refers to the process whereby both the source and target languages are deemed equally important in the research endeavour. It is often used together with back-translation (Beck, Bernal, & Froman, 2003; Brislin, 1970). Necessary adjustments including item localising as discussed in next section were made to both English and Malay Language versions until the final versions of both languages were produced.

5.4.1 Items Localising

This study collected data from employees of Malaysian public universities at all levels who mostly were Malaysian citizens. The questionnaire items were localized to make it easier for them to understand the items. This is because some terms in the original items could not directly apply to Malaysian context. In order to localize the items, an analysis on ISPs documents from four organizations, which is Universiti Malaysia Pahang (UMP)(UMP, 2015), Universiti Kebangsaan Malaysia (UKM, 2016),

Kementerian Pelajaran Tinggi (KPT) (KPT, 2016) and Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) (MAMPU, 2010) were performed to obtain the best terms to be used in the questionnaire. The ISPs from MAMPU and KPT were selected because these two organizations are the main references to Malaysian public universities in developing their own ISPs (UMP, 2015).

Specifically, this analysis was to identify specific terms used in Malaysian ISP documents. The reason is most of the items were adopted and adapted from studies conducted outside of Malaysia. Items that matched were retained, and any term and wording in the items not matching the terms used in these ISPs were changed. Table 5.2 shows the results of the most concerned terms.

Table 5.2 Terms used in Malaysian ISPs

Original Terms	**UMP's ISP**	**UKM's ISP**	**KPT's ISP**	**MAMPU's ISP**
ISP	Dasar Keselamatan ICT	Dasar Keselamatan ICT	Dasar Keselamatan ICT	Dasar Keselamatan ICT
Information Assets	Aset ICT	Aset ICT	Aset ICT	Aset ICT
Information Security	Keselamatan Maklumat	Keselamatan Maklumat	Keselamatan Maklumat	Keselamatan Maklumat
Computer Resources	Sumber ICT	Sumber ICT	NA	Sumber ICT
Computer Security	Keselamatan Komputer	NA	Keselamatan Komputer	Keselamatan Komputer

Based on the analysis, the terms in questionnaire items were changed as shown in Table 5.3.

Table 5.3 Terms to be used in the questionnaire

Terms	**English Version**	**Malay Version**
ISP	ICT Security Policy	Dasar Keselamatan ICT
Information Assets	ICT Assets	Aset ICT
Information Security	Information Security	Keselamatan Maklumat
Computer Resources	ICT Resources	Sumber ICT
Computer Security	Computer Security	Keselamatan Komputer

Nevertheless, some terms remained the same to produce the best items easily understood by respondents. For example, most Malaysian organizations particularly public universities used the term "ICT" (Information and Communication Technology)

for the translation of "information" in the context of Information Technology. However, it is applied to certain terms only. For example, "Information Security Policy" is translated to "Dasar Keselamatan ICT" but "Information Security" is still reffered to as "Keselamatan Maklumat" not "Keselamatan ICT". Series of pre-tests were carried out to ensure that these questionnaire items reach a satisfactory level of reliability on conceptual and measurement equivalence (Sin, Cheung, & Lee, 1999).

5.5 Demographic Variables

Demographic variables of interest for this research are age, gender, working experience, highest education, profession and service type in the organization. This demographic information was used to determine if significant individual demographic differences existed among the respondents or they acted as control variables.

5.6 Control Variables

Review in Section 2.11.7 (Chapter 2) revealed mixed findings on the effects of particular control variables (CV) towards employee's ISP compliance intention (INT) construct. Since the respondents were Malaysian public universities' employees from all levels with various characteristics, there are possibilities that these characteristics influenced INT. Failure to isolate control variables leads to potential confound in the interpretation of data analysis, which could be a threat to internal validity (Brewer, 2000). Moreover, prior studies in ISP compliance literature found that these individual characteristics such as age, gender, working experience, highest education, profession and service type are related to security policy compliance intention.

However, for this research, these variables were considered as variables inexplicitly linked to the hypotheses in the research model and theories of which the model was built on. Thus, in order to control the effects of particular variables from influencing dependent variable, age, gender, working experience, highest education, profession and service type variables were controlled in this study. The purpose was to control the effect of these variables that could potentially influence employee's ISP compliance intention (INT).

5.7 Pre-Test

Although most items in the questionnaires were adopted and adapted from previous studies, series of pre-tests were conducted to ensure the validity for context of this study.

In the first stage, two groups of expert in the field of Information Security Management and Information System were selected to run the pre-test. The first group consisted of director and deputy director of Center of Information Technology from three selected Malaysian public universities. Interview session was conducted with each expert using draft survey questionnaire to see whether the items were appropriately measure the particular constructs. These experts also examined appropriateness of the terms used in Bahasa Malaysia from back-translation stage. Among the comments were in terms of the comprehensiveness of items used to measure a construct and the redundancy of items in measuring a particular construct. They also agreed with some terms used in Bahasa Malaysia's version of questionnaire such as "Dasar Keselamatan ICT" and "Aset ICT". All the input and suggestions in this process were used to improve the items. Items were added, reworded and deleted during the pre-test.

The second group of experts consisted of Information System and Information Technology lecturers who possesed at least PhD from three selected public universities. They also have the experienced conducting survey research methodology, positivist methodology and using SEM techniques and application. This particular group was been assigned to validate the questionnaire items in terms of face validity focusing more on theoretical and practical design of the survey. All suggestions were considered and certain items of the survey as well as design of the survey were revised. One of the experts recommended to add new item for each three-item construct to increase reliability and validity.

The improved version of the questionnaire then was pre-tested by a target group of 20 participants from one department at a selected university to check whether the materials were understandable, clear, and appealing. The test was conducted in interview format whereby the participants were given the questionnaires to answer. The participants' reactions in answering each question were observed and recorded. They were asked directly to identify the problems faced in answering the questions. They

were also allowed to ask and discuss any matter pertaining to the questions with the researcher. All input were then used to refine measurement items before they were administered in the actual study.

Most respondents have shown little difficulty and confusion to answer items of Attitude construct. The reason was these items together with Self-efficacy applied different scale from other construct as discussed in Section 5.3. Specifically, the respondents were confused at first when it came to the items of this construct because the questionnaire asked four similar questions. The respondents were confused and suggested that there were mistakes in the questionnaire without realizing that they actually had to respond to four different scales for those same four questions. Some even suggested that the researcher changed the format of measurement for this construct to be similar like the others. After consulting an expert, items for Attitude were altered to strongly disagree until strongly disagree scale. Although, this was originally performed to reduce CMV effects, due to respondents' responses in this pre-test, it should be performed to reduce ambiguity for the respondents. In fact, reducing ambiguity in the scale items by conducting pre-tests could reduce CMV effects (Podsakoff et al., 2012). However, Self-Efficacy's items were not altered because the respondents were able to clearly identify the scale and managed to answer accordingly. Finally, some new items were introduced as recommended by the experts.

5.8 Pilot Study

The improved version of survey questionnaire was pilot tested to respondents from Universiti Malaysia Pahang (UMP). The respondents were contacted through e-mail to participate in the survey. The survey was distributed and allowed to respond within three weeks time and managed to get 92 responses. After data screening to check for outliers and missing value items, only 87 were available to be used for data analysis. Specifically, sample size calculation for this pilot study employed statistical power and effect size as suggested by Hair et al. (2014) and recommended by Cohen (1992). This rule takes a number of maximum arrows pointing to a construct in the model, significance level and R^2 into consideration in calculating minimum sample size. In research model, since the maximum arrow pointed at ISC is 7, a minimum sample size of 80 is required to achieve statistical power of 80% for detecting R^2 values of at least

0.25 (with a 5% probability of error (Cohen, 1992). Therefore, 87 samples were appropriate for this study.

As for data normality, the results from normality test suggested that the collected data was not multivariate normal. Therefore, the result justifies the use of SmartPLS (Ringle et al., 2015) in this study, which was a non-parametric analysis software.

Table 5.4 shows respondents' profile involved in the pilot study. The table shows a fair distribution of gender, with the majority of them being Malay. Most of the respondents worked as academics, followed by administration and management employees. Majority of them had a Bachelor Degree or higher and had more than five years experience working at the university. Overall, their demographic profiles show the sample consists of appropriate sampling across the selected university.

Table 5.4 Respondents' Profile in Pilot Study

Demographic profile		**n=87**	**Valid percentage (%)**
Gender:	Male	39	44.8
	Female	48	55.2
Age:	18 - 24	2	2.3
	25 - 34	37	42.5
	35 - 44	38	43.7
	45 - 54	9	10.3
	55 and above	1	1.1
Race:	Malay	80	92
	Chinese	4	4.6
	Indian	1	1.1
	Others	2	2.3
Highest Education:	PhD	23	26.4
	Masters	18	20.7
	Bachelor Degree	27	31
	Diploma	10	11.5
	College	5	5.7
	Secondary School	4	4.6
Work experience:	Less than 2 Years	13	14.9
	2 to 5 Years	20	23
	5 to 10 Years	22	25.3
	10 to 20 Years	31	35.6
	20 Years and over	1	1.1
Service Type:	Academic	36	41.4
	Management	24	27.6
	Administration/Support	27	31

5.8.1 Results and Analysis of Pilot Study

The main objective of this pilot study is to test the reliability and validity of measurement items before conducting the actual study. Before conducting further analysis on the collected data, Common Method Bias (CMB) or Common Method Variance (CMV) was examined. To test this bias, Harman's Single-Factor Test (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003) was performed. An unrotated factor analysis of the study items yielded seven factors, the largest of which accounted for 47.551% of the variance. As additional test, correlation matrix procedure (Bagozzi et al., 1991) was performed to identify any highly correlated constructs ($r > 0.9$). The results indicates that all constructs had correlations below the threshold. Thus, results of these two tests prove that CMV bias was not a serious threat in the study.

5.8.2 Measurement Model Assessment

Quality of measurement model that includes all first-order constructs and second-order construct of ISC concept were assessed to ensure the validity and reliability of measurements. The results in Table 5.5 show that CR was greater than 0.80 (Chin, 2010) and AVE for each construct was greater than 0.50 (Nunnally & Bernstein, 1994). These suggest that the measurement model is acceptable. In terms of factor loading, all items were loaded highly on their own latent variable; thus, all measurements had satisfactory levels of reliability. Analysis of discriminate validity using Heterotrait-Monotrait ratio of correlations (HTMT) shows that all values were below 0.90 (Henseler et al., 2015). Cross-loadings also show that indicator loadings were higher than all of its cross loadings (Hair, Ringle, & Sarstedt, 2011). These two criteria indicate that discriminant validity was established for all reflective constructs in the model.

Repeated indicator approach with Mode A and path weighting scheme were employed for ISC second-order construct in order to model second-order factors in PLS analysis. Path weighting scheme is a structural model weighting schemes recommended by Hair et al. (2014). Meanwhile, repeated indicator approach is able to estimate latent variables simultaneously instead of estimating higher and lower order constructs separately (Tehseen & Gadar, 2017). Formative type models are commonly estimated by using Mode A for repeated indicators, in the case of first-order constructs are

reflective (Chin, 2010; Hair, Sarsted, Ringle, & Guderga, 2018; Ringle, Sarstedt, & Straub, 2012).

Table 5.5 Convergent Validity (Pilot Study)

Construct	Item	Loading	CR	AVE
Procedure Countermeasures	PCM1	0.814	0.932	0.775
	PCM2	0.884		
	PCM3	0.943		
	PCM4	0.875		
Risk Management	RM1	0.929	0.927	0.762
	RM2	0.876		
	RM3	0.801		
	RM4	0.881		
Security Education, Training & Awareness	SETA1	0.924	0.951	0.83
	SETA2	0.940		
	SETA3	0.868		
	SETA4	0.909		
Top Management Commitment	TMC1	0.948	0.975	0.906
	TMC2	0.968		
	TMC3	0.960		
	TMC4	0.930		
Monitoring	MON1	0.852	0.938	0.792
	MON2	0.879		
	MON3	0.927		
	MON4	0.899		
Information Security Knowledge	ISK1	0.931	0.960	0.827
	ISK2	0.908		
	ISK3	0.880		
	ISK4	0.913		
	ISK5	0.916		
Information Security Knowledge Sharing	ISKS1	0.823	0.921	0.700
	ISKS2	0.829		
	ISKS3	0.879		
	ISKS4	0.911		
	ISKS5	0.729		
Attitude	ATT1	0.953	0.980	0.924
	ATT2	0.971		
	ATT3	0.961		
	ATT4	0.960		
Normative Belief	NB1	0.953	0.966	0.905
	NB2	0.962		
	NB3	0.939		
Self-Efficacy	SE1	0.948	0.971	0.919
	SE2	0.980		

Table 5.5 continued

Construct	Item	Loading	CR	AVE
	SE3	0.948		
Intention to Comply	INT1	0.941	0.976	0.910
	INT2	0.950		
	INT3	0.962		
	INT4	0.962		

Repeated indicator approach with Mode A and path weighting scheme were employed for ISC second-order construct in order to model second-order factors in PLS analysis. Path weighting scheme is a structural model weighting schemes recommended by Hair et al. (2014). Meanwhile, repeated indicator approach is able to estimate latent variables simultaneously instead of estimating higher and lower order constructs separately (Tehseen & Gadar, 2017). Formative type models are commonly estimated by using Mode A for repeated indicators, in the case of first-order constructs are reflective (Chin, 2010; Hair, Sarsted, Ringle, & Guderga, 2018; Ringle, Sarstedt, & Straub, 2012).

The results of all seven path weights were significant, indicating that each first-order construct makes a unique contribution to second-order construct. The variance inflation factors (VIF) values for all ISC dimensions ranged from 1.95 to 3.75, which were below than 5; thus, indicating satisfactory reliability (Hair et al., 2014). The results therefore, do not indicate multi-collinearity problem and support the formative nature of ISC.

5.8.3 Procedural Remedies of Common Method Bias

All results attain in this pilot study suggested that the survey instrument is capable to collect data in assessing the measurement and structural model. However, some issues in terms of common method bias (CMB) or common method variance (CMV) emerged. Although the survey instrument had passed Harman's Single-Factor Test, CMV assessment using Unmeasured Latent Marker Construct (ULMC) (Chin, Thatcher, & Wright, 2012) showed that there were slightly CMV effects in the data collected. Therefore, some modifications in terms of procedural remedies were conducted to the questionnaire design. In order to incorporate methodological separation and disconnect possible connection between IV and DV (Podsakoff et al.,

2003; Tehseen, Ramayah, & Sajilan, 2017), two Likert scale points were used. For all IVs and DV of INT, seven-point Likert scale was retained but for IV of ATT, NB and SE were changed to five-point Likert scale. The use of different pages for each questionaire section and topic also provide proximal separation and increase physical distance between measures (Podsakoff et al., 2012) as there were seven pages and six sections used in the on-line survey questionnaire.

The survey is not collect any personal information such as email or telephone number to guarantee the anonymity of respondents and confidentiality of their responses (Chang, van Witteloostuijn, & Eden, 2010). This mitigates self-serving answers and the probability that respondents provided answers they believed were expected (Degirmenci, Guhr, & Breitner, 2013; Uffen, Guhr, & Breitner, 2012). Additionally, seven new items of Social Desirability (Fischer & Fick, 1993) were introduced as Measured Latent Marker Variable (MLMV) in order to detect and control CMV effect in data analysis stage as recommended by (Podsakoff et al., 2003). The measure of this construct factor was used to represent CMV in this study (Tehseen et al., 2017). The MLMV could also be used effectively in detecting straight lining in the collected data. The straightline answers for MLMV items indicate potential straight lining issue in the respective responses. The final survey instrument is shown in Appendix G.

5.9 Chapter Summary

This chapter has discussed the development of research instruments used in measuring constructs in the research model. Although most of the items were adopted and adapted from previous validated studies, all these items still need to be localized to be used in this research context. All the process including items translation, identifying demographic variables and control variables as well as series of pre-tests and pilot test were discussed in this chapter. As a result, validated survey questionnaire for the actual data collection was produced as in Appendix G. The next chapter discusses the results and analysis of the collected data.

CHAPTER 6

FINDINGS AND DISCUSSION

6.1 Introduction

Previous chapter has discussed the development of research instrument to collect data for research model validation. Therefore, this chapter continues to present and discuss the findings and analysis of the collected data, model validation as well as the hypotheses testing for this research. It consists of thirteen main sections. The next two sections present results of data collection followed by results of screening process. The evaluation of Common Method Bias (CMB) is discussed in section four. Section five provides a general description of survey respondents. Descriptive statistics and normality tests for the collected data are discussed and presented in section six and section seven respectively. Then, assessments of measurement model is discussed in section eight followed by assessments of ISC concept as multidimensional second-order construct in section nine. Section ten reports the results of structural model and followed by results of hypotheses testing in section eleven. Discussions on the findings is presented in section twelve. Finally, a short summary concludes this chapter in section thirteen.

6.2 Data Collection Results

According to the research model, the maximum number of arrowheads pointing at ISC is the highest, which is 7; therefore, the minimum sample for this study is 70 x 10 = 70. Meanwhile, by using G*power program (Faul et al., 2009) for minimum sample size, 153 observations are needed to achieve statistical power of 95% for medium effect size of 0.15 with 5% probability of error. However, in MIS research that uses SEM technique, since 44 items were included in the survey questionnaire, 440

samples are required for this study based on recommendation by Westland (2010) who suggested the use of 10 cases per indicator. Since data collection process managed to obtain 634 responses as mentioned in Section 4.7.2 (Chapter 4), therefore, 634 sample size is considered as appropriate sample size for this study.

6.3 Data Screening Results

Data screening process detected as many as five (5) straight lining responses from 634 responses collected in data collection phase. In addition, by using IBM SPSS Statistics 22 software package, as many as 24 outliers were detected and one duplicate data case was detected. All these invalid responses including one response for the duplicate case were removed from the sample. The final number of valid responses is 604.

There are some missing values in demographic and Marker Variable (MV) sections. For demographic data, missing value only recorded by data field of Profession, which is three responses (0.50%) only. As for MV responses, the missing values are as shown in Table 6.1. The table indicates the missing value for this MV is also too small with below than 1%. Overall, the screening process found that there is a minimal amount of missing data (less than 5%). According to Cohen and Cohen (1983), missing data up to 10% may not cause any serious problem in the interpretation of the findings. As for the treatment of missing data for marker variable, mean replacement was used as recommended by Hair et al. (2014).

6.4 Controlling Common Method Bias

According to Podsakoff and Organ (1986), data collected from a single source for both independent and dependent variables would have the possibility to contain Common Method Bias (CMB) or Common Method Variance (CMV). In this research, besides establishing procedural remedies as discussed in Section 5.8.3 (Chapter 5), statistical remedies was also conducted to detect and control possible CMV effects.

6.4.1 Correlation Matrix Procedure

Correlation matrix was examined as the first test to detect CMV in the data collected. Table 6.2 shows that the correlation between constructs are below 0.90 which

indicates that no initial evidence of possible common method bias was presence (Bagozzi, Yi, & Phillips, 1991).

Table 6.1 Missing Value in Marker Variable Items

Items	N	No. of Missing Value	Percentage of Missing Value (%)
SD1	604	0	0
SD2	604	0	0
SD3	603	1	0.17
SD4	604	0	0
SD5	601	3	0.50
SD6	602	2	0.33
SD7	602	2	0.33

6.4.2 Harman's Single-Factor Test

Harman's Single-Factor test was conducted as the second test to examine CMV. An unrotated factor analysis of all study items yielded nine factors together accounted for 79.8 percent of the total variance, the largest of which accounted for 44 percent of the variance as shown in Appendix C. Given that no single factor solution emerged and no general factor accounted for most of the variance, CMV was not viewed as a significant threat in this research (Podsakoff & Organ, 1986).

6.4.3 Partialling Out a "Marker" Variable

To confirm both assessments, Partialling Out a "Marker" Variable using Podsakoff et al. (2003) method was conducted. Figure 6.1, Figure 6.2, Figure 6.3 and Figure 6.4 shows results of R^2 at ATT, NB, SE and INT after marker variable introduced on each endogenous construct.

Table 6.3 shows that changes in R^2 were below than 10 percent before and after marker variable was added into each construct (Podsakoff et al., 2003). This suggests that there is no substantial common method bias in the samples collected for this study.

Table 6.2 Correlations between Constructs

Construct	1	2	3	4	5	6	7	8	9	10	11
1. PCM	1										
2. RM	0.570	1									
3. SETA	0.577	0.613	1								
4. TMC	0.554	0.685	0.756	1							
5. MON	0.455	0.586	0.589	0.606	1						
6. ISK	0.540	0.728	0.730	0.767	0.675	1					
7. ISKS	0.481	0.534	0.570	0.626	0.526	0.628	1				
8. ATT	0.342	0.363	0.262	0.417	0.261	0.378	0.390	1			
9. NB	0.405	0.402	0.439	0.512	0.370	0.499	0.476	0.529	1		
10. SE	0.295	0.247	0.356	0.303	0.247	0.358	0.412	0.241	0.358	1	
11. INT	0.431	0.471	0.351	0.490	0.312	0.446	0.483	0.596	0.524	0.380	1

Table 6.3 Results of Partialling Out a Marker Variable

Dependent Variable	Before Marker Introduced (R^2)	After Marker Introduced (R^2)	Percentage Change (%)
Attitude	0.182	0.199	9.34
Normative Belief	0.303	0.307	1.32
Self-Efficacy	0.155	0.160	3.23
Intention to Comply	0.449	0.471	4.90

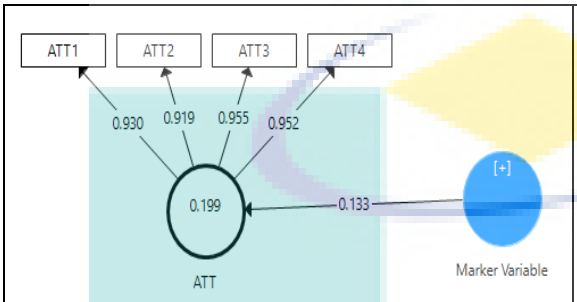


Figure 6.1 Marker Variable on ATT

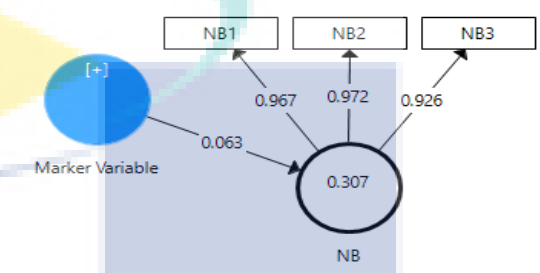


Figure 6.2 Marker Variable on NB

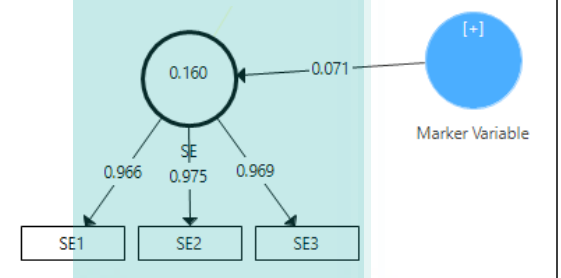


Figure 6.3 Marker Variable on SE

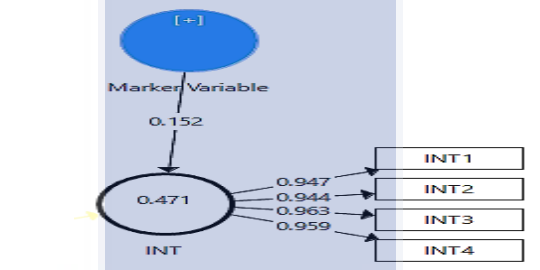


Figure 6.4 Marker Variable on INT

6.5 Profile of Respondents

Table 6.4 presents profile of respondents. The samples consist of 604 respondents with the majority are Malays (91.6%). Meanwhile, those who are Chinese and Indian made of 2.2% and 1.2% respectively of the sample. Interestingly, the table shows that other race was recorded at 5.1% which consisted of races such as Kadazan, Bidayuh and other nationality such as Pakistan, Algeria, Myanmar and other countries. This percentage is appropriate since majority of employees in Malaysian public universities are Malays followed by combination of races such as Chinese, Indian and others in Malaysia as well as academics from other countries.

Generally, gender for the sample comprises of 59.6% female and 40.4% male which was a normal tabulation for this sector because normally female employees were more than male. Meanwhile, most of the respondents' age was in the range of 35 – 44

years old (45.2%), followed by 25 -34 years old (31.1%) and 45 – 54 years old (19.5%). Those in the range of 55 years old and above were recorded at only 3.5%. This percentage was also normal since employees in this range were those close to retiring age as set up by the universities. Finally, respondents' whose age in the range of 18 – 24 years old was the least responded to the questionnaire with 0.7%. Although it seems abnormal, the reality was employees in this range of age was only a few. Common starting working age for employees is at 24 and above since most Malaysian finish their study especially for bachelor level is at this age.

Additionally, certain responses suggested that employees who had less than one year working experience were reluctant to participate in this survey. In fact, the reseacher received several e-mails from this type of respondents stating that they did not want to get involved in this survey. They gave "still learning and adapting; therefore, do not want to evaluate the university" as their main reason.

Meanwhile, item on working experience indicates that most of them had 10 – 20 years working experience followed by 5 – 10 years. These two categories formed more than 65% of the total samples. As for service type, nearly half of total respondents were academician and more than half of the respondents were the combination of non-academic employees such as administration, support and management employees. Nevertheless, considering that the management employees could also consist of academicians such as those who were appointed as Deans, Directors and other management positions in the university, it could be concluded that majority of the respondents were academic employees.

Additionally, more than 75% of the respondents had Bachelor Degree and above with most of them had PhD (30.3%). This appropriately represents this sector since most of academic and non-academic employees possess Degree and above for academic qualification. This is consistent with result on service type whereby most respondents were academicians; and most academicians in Malaysian public universities have Masters and PhD. Finally, most respondents (80.8%) considered themselves as non-IT professional and only 18.7% were IT professional. Three respondents with 0.5% did not state their answers for this question.

Table 6.4 Profile of Respondents

Demographic profile	n=604	Percentage (%)
Gender:		
Male	244	40.4
Female	360	59.6
Age:		
18 - 24	4	0.7
25 - 34	188	31.1
35 - 44	273	45.2
45 - 54	118	19.5
55 and above	21	3.5
Race:		
Malay	553	91.6
Chinese	13	2.2
Indian	7	1.2
Others	31	5.1
Highest Education:		
PhD	183	30.3
Masters	172	28.5
Degree	111	18.4
Diploma	75	12.4
STPM/College	26	4.3
SPM	37	6.1
Work experience in the university:		
Less than 2 Years	52	8.6
2 to 5 Years	85	14.1
5 to 10 Years	176	29.1
10 to 20 Years	220	36.4
20 Years and over	71	11.8
Service Type:		
Academic	294	48.7
Management	94	15.6
Administration/Support	204	33.8
Academic & Management	9	1.5
Academic & Management & Administration/Support	3	0.5
Profession:		
IT Professional	113	18.7
Non-IT Professional	488	80.8
Missing	3	0.5

Table 6.5 shows the number and percentage of respondents based on universities. In general, the samples contain respondents from each public university

available in Malaysia with the exception of Universiti Malaysia Pahang (UMP) and Universiti Sultan Azlan Shah (USAS). Respondents from UMP were excluded from actual data collection since they already participated in pilot study. USAS was also excluded since their official website did not provide list of staff name and their email (from September until December 2017). List of universities in the table was sorted based on Malaysian Public Universities ranking in 2017 provided by Ranking Web of Universities (2017). The table shows that the highest number of respondents are from four Malaysian top five universities, which are Universiti Malaya (UM), Universiti Sains Malaysia (USM), Universiti Putra Malaysia (UPM) and Universiti Kebangsaan Malaysia (UKM). This indicates that the samples do not only comprise of most Malaysian public universities but also comprises appropriate number of respondents from Malaysian renowned universities. Although the number of respondents from Unisza and UPNM are relatively small, their responses were still accepted for analysis because they also represented the population under study. Furthermore, there is no analysis based on universities was conducted in this research.

Table 6.5 Number of Respondent based on Universities

No.	University	No. of Respondents	Percentage (%)
1	Universiti Malaya (UM)	45	7.5
2	Universiti Teknologi Malaysia (UTM)	31	5.1
3	Universiti Sains Malaysia (USM)	52	8.6
4	Universiti Putra Malaysia (UPM)	48	7.9
5	Universiti Kebangsaan Malaysia (UKM)	48	7.9
6	Universiti Teknologi MARA (UiTM)	40	6.6
7	Universiti Islam Antarabangsa Malaysia (UIAM)	45	7.5
8	Universiti Malaysia Perlis (UniMAP)	26	4.3
9	Universiti Utara Malaysia (UUM)	45	7.5
10	Universiti Tun Hussein Onn Malaysia (UTHM)	21	3.5
11	Universiti Malaysia Sabah (UMS)	26	4.3
12	Universiti Malaysia Sarawak (UNIMAS)	37	6.1
13	Universiti Teknikal Malaysia Melaka (UTeM)	27	4.5
14	Universiti Malaysia Terengganu (UMT)	33	5.5
15	Universiti Pertahanan Nasional Malaysia (UPNM)	8	1.3
16	Universiti Pendidikan Sultan Idris (UPSI)	12	2.0
17	Universiti Malaysia Kelantan (UMK)	26	4.3
18	Universiti Sains Islam Malaysia (USIM)	29	4.8
19	Universiti Sultan Zainal Abidin (UniSZA)	5	0.8
Total		604	100

6.6 Descriptive Statistics for the Main Constructs

Descriptive statistics in terms of mean, standard deviation as well as skewness and kurtosis for 7-point and 5-point Likert scales items of the main variables used in this research is as in Appendix D and Appendix E respectively. For 7-point Likert scale, mean for all items of ISC dimensions are in the range of 4.7 to 6.0 except for RM3, whereas mean for INT is in the range of 6.0 to 6.2. As for 5-point scale, mean values for three constructs of behavioral factors of ATT, NB and SE are in the range of 3.6 and 4.7.

Skewness and kurtosis were used to check normal distribution of the data. According to Kline (2011), variables with values of skew index (SI) > ±3 are seen as extremely skewed, wherein the sign of SI indicates direction of the skew. Kline (2011) also suggested that variables with values of kurtosis index (KI) > ±10 suggest a problem. Referring to skewness and kurtosis data results in Appendix E, no item exhibited significant skew or kurtosis. Therefore, data collected are univariately normally distributed.

6.7 Normality Test

To attain more details on normality of the collected data, all latent variables scores were examined using software available at: https://webpower.psychstat.org/models/kurtosis/results.php?url=fb9771ad65087c96bdc6a313929fa338 as recommended by Cain, Zhang, and Yuan (2016). The results are depicted in Appendix F. The results suggest univariate skewness and kurtosis value for each construct is in the range of cut-off value of > ±3 and > ±10 respectively (Kline, 2011). This suggests that the data is normally distributed. However, Mardia's multivariate skewness and Mardia's multivariate kurtosis show the collected data was not multivariate normal. Therefore, it justifies the use of SmartPLS in this research, which is a non-parametric analysis software.

6.8 Measurement Model Assessment

Following the widely adopted two-step approach to structural equation modeling (Anderson & Gerbing, 1988; Hulland, 1999), quality of the measurement model for all

first-order constructs including ISC dimensions was assessed beforehand to ensure the validity and reliability of the measurements.

6.8.1 Reflective Measurement Model Assessment

Figure 6.5 shows the result of PLS Algorithm extracted from SmartPLS software. It shows that all outer loadings exceed than 0.708 except for RM3. Thus, special attention was put on this item in deciding whether to retain this item or not. Although AVE for this particular construct is more than 0.5, assessment on cross-loadings revealed that this item's outer loading on RM construct is not greater than 0.1 on all of its loadings on other constructs (Hair et al., 2013) as indicated in Appendix H. Therefore, this item was deleted from the model at both RM construct and ISC construct. Then, PLS algorithm was run again without this problematic item and measurement model was assessed once again.

Figure 6.6 shows PLS algorithm result after removing RM3 item. It shows that all items' outer loadings exceed the value of 0.708. Therefore, the assessment process to evaluate measurement model proceeded as intended.

The first criterion is to assess reliability of the measurement model. Table 6.6 shows the results of Cronbach Alpha (α) and Composite Reliability (CR). It shows that all values exceed the cut-off value for Cronbach Alpha and CR, which are 0.70 and 0.80 respectively. Therefore, the results of these two assessments show that all measurements have good reliability in measuring the constructs.

The second criterion of measurement model assessment is convergent vality. As shown in Table 6.7, all factor loadings exceed 0.708 and Average Variance Extracted (AVE) for each construct exceeds 0.50 (Hair et al., 2014). These suggest convergent validity for measures of all constructs were established and the measurement model is acceptable.

The last criterion assessed in measurement model assessment was discriminant validity. At the item level, Appendix I shows that each item was loaded highest on its respective latent construct and at least greater than 0.10 on items of other constructs (Hair et al., 2013) and this indicates that all measurement items show acceptable discriminant validity.

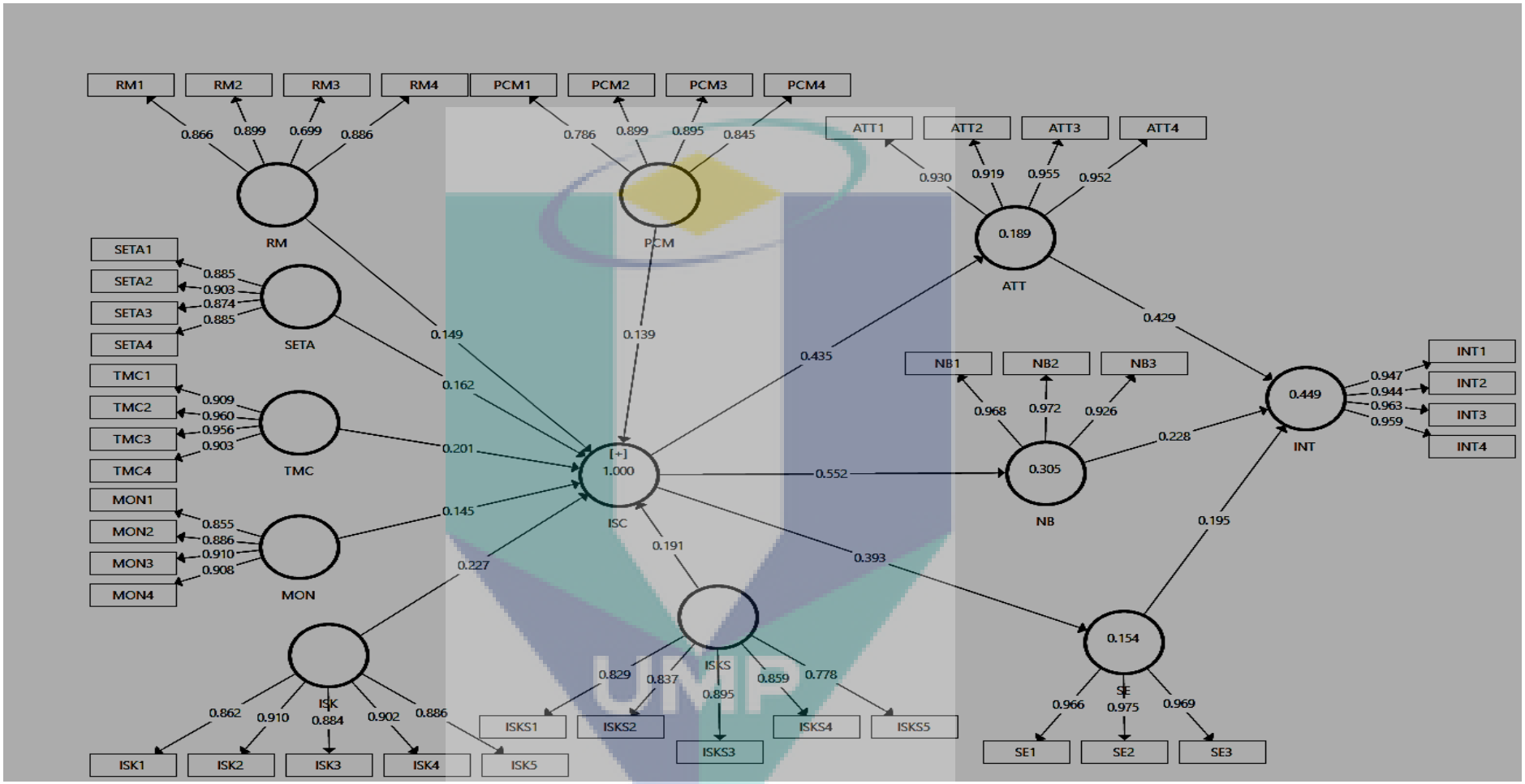


Figure 6.5 PLS Algorithm Result

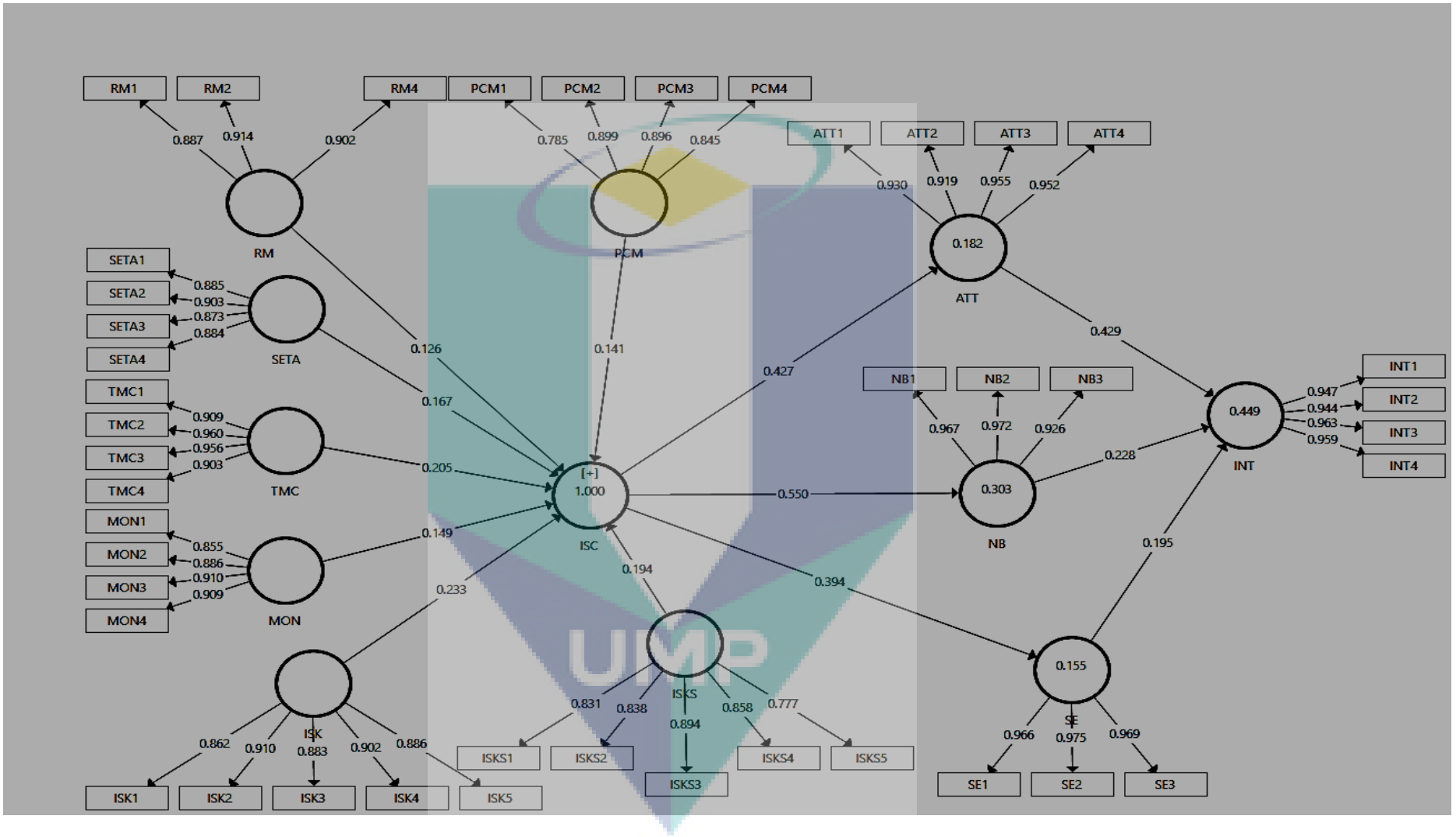


Figure 6.6 PLS Algorithm without RM3 item

Table 6.6 Internal Consistency Reliability

Construct	Cronbach Alpha	CR
Procedure Countermeasures	0.879	0.917
Risk Management	0.884	0.928
Security Education, Training and Awareness	0.909	0.936
Top Management Commitment	0.950	0.964
Monitoring	0.913	0.939
Information Security Knowledge	0.934	0.950
Information Security Knowledge Sharing	0.896	0.923
Attitude	0.955	0.968
Normative Belief	0.952	0.969
Self-Efficacy	0.968	0.979
Intention to Comply	0.967	0.976

Table 6.7 Convergent Validity Results

Construct	Item	Loading	AVE
Procedure Countermeasures	PCM1	0.785	0.735
	PCM2	0.899	
	PCM3	0.896	
	PCM4	0.845	
Risk Management	RM1	0.887	0.812
	RM2	0.914	
	RM4	0.902	
Security Education, Training and Awareness (SETA)	SETA1	0.885	0.786
	SETA2	0.903	
	SETA3	0.873	
	SETA4	0.884	
Top Management Commitment	TMC1	0.909	0.869
	TMC2	0.960	
	TMC3	0.956	
	TMC4	0.903	
Monitoring	MON1	0.855	0.792
	MON2	0.886	
	MON3	0.910	
	MON4	0.909	
Information Security Knowledge	ISK1	0.862	0.790
	ISK2	0.910	
	ISK3	0.883	
	ISK4	0.902	
	ISK5	0.886	
Information Security Knowledge Sharing	ISKS1	0.831	0.706
	ISKS2	0.838	
	ISKS3	0.894	

Table 6.7 continued

Construct	Item	Loading	AVE
	ISKS4	0.858	
	ISKS5	0.777	
Attitude	ATT1	0.930	0.882
	ATT2	0.919	
	ATT3	0.955	
	ATT4	0.952	
Normative Belief	NB1	0.967	0.913
	NB2	0.972	
	NB3	0.926	
Self-Efficacy	SE1	0.966	0.941
	SE2	0.975	
	SE3	0.969	
Intention to Comply	INT1	0.947	0.909
	INT2	0.944	
	INT3	0.963	
	INT4	0.959	

Note: RM3 was deleted due to low factor loading

As for the construct level, as shown in Table 6.8, square root of each AVE is greater than the correlations between constructs, indicating that more variance is shared between the construct and its indicators than with any other constructs (Fornell & Larcker, 1981). Moreover, analysis of HTMT in Table 6.9 shows all values of reflective constructs were below 0.90 and these indicate the discriminant validity was established to all reflective constructs in the model (Henseler et al., 2015). Based on these three assessments of reflective items and constructs, the requirements for discriminant validity were satisfied.

6.8.2 Summary of Reflective Measurement Model Evaluation

Results of reflective measurement model assessments suggest that internal consistency (composite reliability), convergent validity and discriminant validity were achieved. All assessments passed measurement criteria discussed in Section 4.8.2.1 (Chapter 4).

Table 6.8 Discriminant Validity using Fornell Larcker Criterion (Fornell & Larcker, 1981)

	PCM	RM	SETA	TMC	MON	ISK	ISKS	ATT	NB	SE	INT
PCM	**0.857**										
RM	0.570	**0.901**									
SETA	0.577	0.613	**0.887**								
TMC	0.554	0.685	0.756	**0.932**							
MON	0.455	0.586	0.589	0.606	**0.890**						
ISK	0.540	0.728	0.730	0.767	0.675	**0.889**					
ISKS	0.481	0.534	0.570	0.626	0.526	0.628	**0.840**				
ATT	0.342	0.363	0.262	0.417	0.261	0.378	0.390	**0.939**			
NB	0.405	0.402	0.439	0.512	0.370	0.499	0.476	0.529	**0.955**		
SE	0.295	0.247	0.356	0.303	0.247	0.358	0.412	0.241	0.358	**0.970**	
INT	0.431	0.471	0.351	0.490	0.312	0.446	0.483	0.596	0.524	0.380	**0.953**

Table 6.9 Discriminant Validity using HTMT Criteria (Henseler et al., 2015)

	PCM	RM	SETA	TMC	MON	ISK	ISKS	ATT	NB	SE	INT
PCM											
RM	0.645										
SETA	0.642	0.682									
TMC	0.603	0.746	0.813								
MON	0.505	0.650	0.645	0.649							
ISK	0.592	0.800	0.791	0.813	0.729						
ISKS	0.539	0.600	0.625	0.678	0.578	0.683					
ATT	0.370	0.395	0.280	0.438	0.278	0.401	0.430				
NB	0.444	0.437	0.472	0.540	0.396	0.529	0.517	0.554			
SE	0.319	0.266	0.379	0.315	0.263	0.374	0.437	0.250	0.373		
INT	0.468	0.510	0.374	0.512	0.331	0.469	0.527	0.620	0.546	0.391	

6.9 Assessment of ISC as a Second-Order Construct

ISC as second-order construct was assessed using repeated indicator approach. For this study, higher-order construct which is ISC was created using the indicators of its lower-order constructs, which are PCM, RM, SETA, TMC, MON, ISK and ISKS as illustrated in Figure 6.7. It is worth to note that since this study employed repeated indicator approach to assess relationships between LOCs and HOC, careful attention should be given to the number of items for each LOCs. Referring to Figure 6.7, although there are differences in the number of item for each construct, the differences are still comparable. This is consistent with Hair et al. (2018) who recommended equal number of indicators or at least comparable across LOCs for using repeated indicator approach. In this research, although ISK and ISKS have more items than other constructs, the difference is just one item compared to the others, which have four items. In fact, Figure 6.6 shows that the weight of ISKS is lower than TMC, even though ISKS has one item more than TMC.

As for RM that has the smallest number of items, the difference is still comparable since majority of LOCs have four items. In fact, the initial number of item for RM is four as shown in Figure 6.5. One item, which is RM3 was deleted due to low loadings. In the case of significant difference in number of items among LOCs, Hair et al. (2018) recommended to assess the effect of indicator elimination on the relationships between HOC and LOCs, particularly if LOCs are measured formatively. Although LOCs in this research were measured reflectively, weight of relationship between RM and ISC did not much changed and still significant before and after RM3 was removed. A bootstrapping procedure was employed using 5000 sub-samples to assess the significance of weights of formative indicators as shown in Figure 6.8. Table 6.10 shows the results of assessment on ISC as second-order construct. The results reveal that indicators' weights were above the value of 0.10 as recommended by Lohmöller (1989). Table 6.10 also reveals that all weights of formative indicators have significant *t*-values. This provides an empirical support to retain all the indicators (Hair et al., 2011). These results suggest that all dimensions formulated and proposed were relevant and significant in contributing to the underlying concept of ISC (Becker et al., 2012; Wetzels, Odekerken-Schröder, & Oppen, 2009; Wright et al., 2012). These findings answer Research Question 3a (RQ3a).

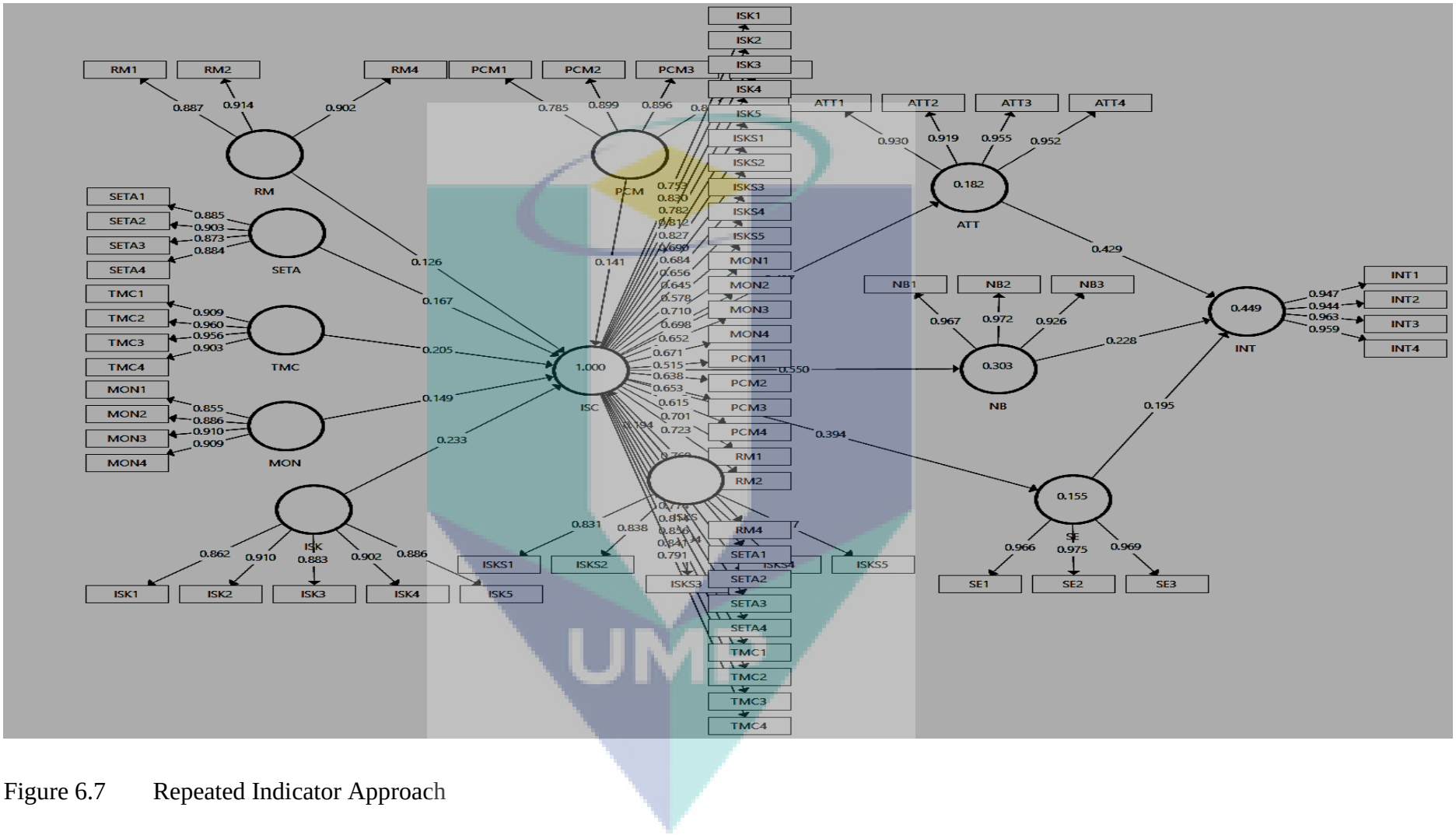


Figure 6.7 Repeated Indicator Approach

Moreover, Table 6.11 shows confidence interval and p-values for formative indicators. It provides additional evidence regarding the significance of weights as 0 did not occur between the higher and lower values of confidence intervals. The results also suggest that ISK is the most important and significant dimension of ISC and this finding answers Research Question 3b (RQ3b). At this point, Research Objective 3 (RO3) was achieved.

Table 6.10 Testing of Significance of Weights

Relationship	Weight/Original Sample (O)	t-value (|O/STDEV|)	p-values
PCM -> ISC	0.141	***22.499	p<0.001
RM -> ISC	0.126	***28.918	p<0.001
SETA -> ISC	0.167	***31.983	p<0.001
TMC -> ISC	0.205	***37.393	p<0.001
MON -> ISC	0.149	***23.737	p<0.001
ISK -> ISC	0.233	***44.299	p<0.001
ISKS -> ISC	0.194	***27.684	p<0.001

Note: Critical t values ***2.33 (significance level= 1%)

Table 6.11 Confidence Interval

Second-Order Construct	Formative Indicators	p-value	Confidence Interval	Significance (p≤0.05)?
ISC	PCM -> ISC	p<0.001	0.131, 0.151	Yes
	RM -> ISC	p<0.001	0.119, 0.133	Yes
	SETA -> ISC	p<0.001	0.158, 0.176	Yes
	TMC -> ISC	p<0.001	0.197, 0.215	Yes
	MON -> ISC	p<0.001	0.139, 0.159	Yes
	ISK -> ISC	p<0.001	0.225, 0.242	Yes
	ISKS -> ISC	p<0.001	0.183, 0.205	Yes

Reliability of ISC as a formative construct was examined by assessing collinearity of indicators, which are the seven formulated dimensions. Table 6.12 shows that VIF value for each construct is below than 5 and this indicates collinearity of the formative constructs does not reach the critical levels (Hair et al., 2014; Hair, Hult, Ringle, & Sarstedt, 2017). This also suggests that each dimension represents a distinct aspect of ISC in contributing to the overall concept of ISC.

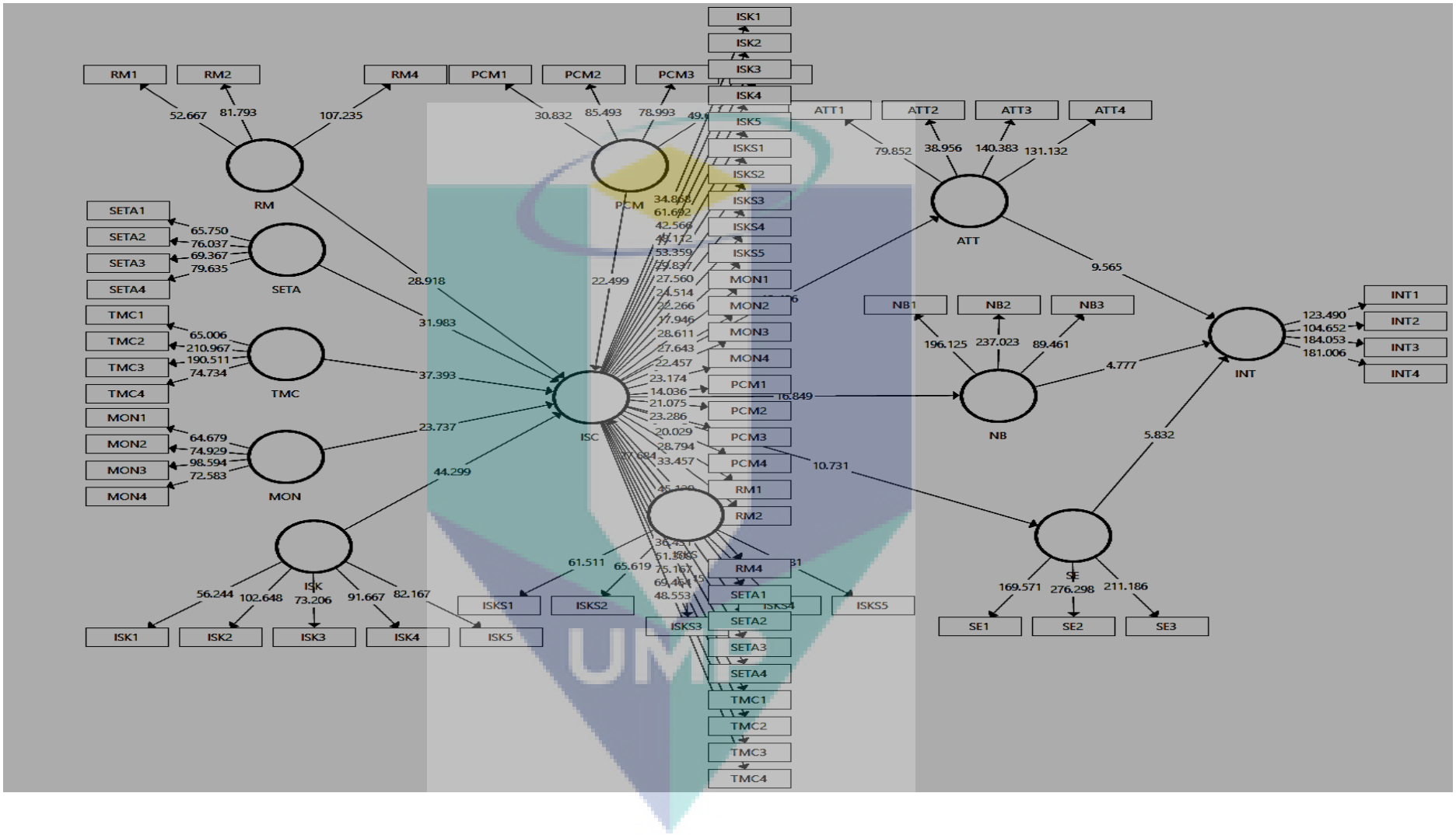


Figure 6.8 Results of Bootstrapping

Table 6.12 VIF Values

Construct	VIF Value
PCM	2.018
RM	2.511
SETA	2.869
TMC	3.375
MON	1.997
ISK	3.698
ISKS	1.875

6.10 Structural Model Assessment

The assessments on measurement model including second-order construct prove that all constructs' measures are reliable and valid. This indicates that analysis of structural model could be proceeded. According to Hair et al. (2014), assessment of the structural model results would determine how well empirical data support the theory/concept and therefore to decide if the theory/concept has been empirically confirmed. In structural model assessment for this study, the relationships between constructs and model's predictive capabilities were examined by estimating path coefficients and R^2 value. In addition, the effect size, f^2, Confidence Interval (CI) and model predictive relevance, Q^2 were also employed as additional analysis to confirm the structural model assessment.

6.10.1 Collinearity Issue

As recommended by Hair et al. (2014), structural model assessment should be started by checking the structural model for collinearity issues. Tolerance (VIF) values below than 5 will indicate no issue of collinearity among constructs in the structural model. Table 6.13 clearly shows that tolerance (VIF) values for all tested relationships are below than 5; thus, it indicates that there is no issue of collinearity among constructs in the structural model.

Table 6.13 Collinearity Assessment

Relationship	VIF
ISC -> ATT	1
ISC -> NB	1
ISC -> SE	1
ATT -> INT	1.395
NB -> INT	1.506
SE -> INT	1.152

6.10.2 Structural Model Path Coefficients

In this study, a path coefficient with 5% or less probability error is considered significant. Since there are recommendations suggesting to report *t*-value in determining the significance of path coefficients, a bootstrapping (resampling = 5000) procedure was performed to calculate *t*-value. For this study, *t*-value of 1.65 (one-tailed) and above is considered significant for relationships hypothesized in the model. According to Hair, Ringle, and Sarstedt (2011), critical *t*-values for one-tailed test are 1.65 ($p<0.05$), and 2.33 ($p<0.01$).

Table 6.14 shows significance of path coefficient (β) values for all relationships hypothesized in this study. In general, results reveal that all relationships are significant with *t*-value more than 2.33 and p-value < 0.01. The results show that ISC significantly influences Normative Belief (NB), Attitude (ATT) and Self-Efficacy (SE) of employees towards ISP compliance in the organization. Of all three behavioral factors, NB was the most affected by ISC followed by ATT and SE. These findings are consistent with Flores and Ekstedt (2016) who found ISC significantly influences NB and ATT but in the context of resisting to social engineering. This suggests that ISC has more influence towards attitude and normative belief rather than improving the skills and ability of an employee in the organization especially in Malaysian public university.

Table 6.14 Structural Model Assessment

Relationship	β	t-value	p-values
ISC -> ATT	0.427	13.426	p<0.001
ISC -> NB	0.550	16.849	p<0.001
ISC -> SE	0.394	10.731	p<0.001
ATT -> INT	0.429	9.565	p<0.001
NB -> INT	0.228	4.777	p<0.001
SE -> INT	0.195	5.832	p<0.001

These three behavioral factors were also significantly influenced employee's ISP compliance intention (INT). These findings consistent with Flores and Ekstedt (2016); and Dugo (2007) but in different context of security behavior. These findings also suggest that ISC has similar effect on employees security behavior in the organization by improving ISP compliance and reducing ISP violation. Interestingly, although ISC has the strongest influence towards NB, however ATT was found as the most influential

factor for INT compared to the three behavioral factors. Similarly, study by Flores and Ekstedt (2016) also found ATT has stronger influence on intention to resist to social engineering compared to NB. Therefore, besides empirically proves that ISC based on seven dimensions influences employees' ISP compliance behavior, the findings also prove that ISC establishment in the organization provides holistic approach in improving security compliance and reducing information security risks.

Among three behavioral factors of ATT, NB and SE, the results show that SE has the weakest relationship with INT. This is consistent with previous studies that found SE has less influence towards INT. However, significant tests reveal that the relationship is significant with *t*-value = 5.832 at p<0.001. In fact, this relationship is relatively stronger with higher significance values than the relationship found in Ifinedo (2014a) and Ifinedo (2012) as shown in Table 2.5 (Section 2.11.4, Chapter 2). Specifically, β values in Ifinedo (2014a) and Ifinedo (2012) is 0.18 (p-value < 0.05) and 0.17 (p-value < 0.01) respectively. Therefore, considering this fact, the relationship between SE and INT is acceptable as it is strong and significant.

6.10.3 Control Variable Effect

As this research also employed several control variables to examine their potential confounding effects on the model, PLS algorithm was performed to the same model with all control variables pointing to INT construct. Bootstrapping procedure was performed to examine the significance of the relationships. Table 6.15 shows the results of path coefficient between all control variables with INT. The result shows that all relationships are not significant at *t*-value more than 1.65 and p<0.05. Therefore, control variables have no significant effects on INT construct.

Table 6.15 Results of Control Variables Effects

	Original Sample	Sample Mean	Standard Deviation	t-value	p-values
Age -> INT	0.021	0.021	0.037	0.553	0.290
Gender -> INT	-0.02	-0.02	0.030	0.688	0.246
Experience -> INT	0.069	0.068	0.042	1.618	0.053
Highest Education -> INT	0.022	0.023	0.050	0.444	0.329
Profession -> INT	0.006	0.006	0.025	0.234	0.407
Service Type -> INT	0.045	0.044	0.046	0.979	0.164

As an additional test, the effect size, f^2 for control variables were examined. Table 6.16 shows the values of f^2 for all control variables. According to Cohen (1988), f^2 values of 0.02, 0.15, and 0.35 indicate that an exogenous construct has small, medium, or large effect, respectively, on an endogenous construct. The table shows that all control variables have no effect on INT construct. This confirms that age, gender, working experience, highest education, profession and service type have no significant effect on dependent variable of INT.

Table 6.16 Effect Sizes of Control Variables

Control Variable	f^2	Effect Size
Age	0.000	No effect
Gender	0.001	No effect
Experience	0.005	No effect
Highest Education	0.000	No effect
Profession	0.000	No effect
Service Type	0.002	No effect

Therefore, all these control variables were excluded in subsequent analysis. Referring back to Section 2.11.7 (Chapter 2), this decision is consistent with prior studies that found age, gender, working experience, highest education, profession and service type have no effects on employees' ISP compliance intention. The decision was also consistent with previous studies that did not use control variable in relation with ISP compliance intention as discussed in that section.

6.10.4 Coefficients of Determination, R^2

Table 6.17 shows R^2 values of endogenous constructs explained by exogenous constructs linked to it. R^2 for main DV, which is INT is 0.449, indicates that variables in the model explained about 45% of the variance in it. In other words, this research found that ISC, ATT, NB and SE could explained 45% of the employees' ISP compliance intention in the Malaysian public university. This suggests that another 55% of the explanation could be explained by another variables that involved in this study.

The R^2 of 45% is high by the standard of structural equation modeling (Hu et al., 2012) and in behavioral research (Hair et al., 2014). This value of R^2 is considered as desirable value in predicting ISP compliance behavior particularly involving ISC construct in the model. For instance, R^2 for main DV in study by D'Arcy and Greene (2014); D 'Arcy and Greene (2009); and Alkalbani et al. (2015) is 0.45, 0.31 and 0.48

respectively. Apart from that, R^2 for INT in this research is also higher compared to R^2 for main DV in prior studies using the same TPB variables, which is 0.417 in Dugo (2007) and 0.42 in Flores and Ekstedt (2016). In summary, considering that the model in this research is solely focusing on ISC compared to other prior models, besides the parsimony of the model, the results of R^2 indicate that this ISC model has high predictive accuracy in predicting ISP compliance behavior.

Table 6.17 Coefficient of Determination, R^2

Construct	R^2
Attitude (ATT)	0.182
Normative Belief (NB)	0.303
Self-Efficacy (SE)	0.155
Intention to Comply (INT)	0.449

Apart from that, R^2 for TPB constructs are in reasonable range with NB has the most amount of variance explained by ISC with 30.3%, followed by ATT and SE with 18.2% and 15.5% respectively. These values are higher compared to prior studies employing similar variables. In the study by Flores and Ekstedt (2016), the R^2 of ATT, NB and SE are 0.19, 0.21 and 0.24 respectively. whereas in Dugo (2007), the R^2 values for ATT and NB are 0.228 and 0.022 respectively. Considering the amount of variance in these two studies is not solely explained by ISC construct, R^2 value for each TPB variable in this current research is considered high and also represented the actual values of variance explained by ISC construct.

6.10.5 Effect Size

The effect size, f^2 allows the assessment of an exogenous construct's contribution to an endogenous latent variable's R^2 value. The f^2 values of 0.02, 0.15, and 0.35 indicate an exogenous construct's small, medium, or large effect, respectively, on an endogenous construct Cohen (1988). Table 6.18 shows the effect size of particular exogenous variables on respective endogenous variables. The results reveal that ISC has large effect on NB and medium effect on ATT and SE. This suggests that ISC has strong effect towards all three employee's behavior factors with the strongest is towards NB followed by ATT and SE.

Table 6.18 Effect Size Results

Path	f^2	Effect size
ISC -> ATT	0.223	Medium
ISC -> NB	0.435	Large
ISC -> SE	0.183	Medium
ATT -> INT	0.239	Medium
NB -> INT	0.063	Small
SE -> INT	0.060	Small

In terms of employee's ISP compliance intention (INT), ATT has medium effect whereas NB and SE have small effect on this construct. This means most of the variance in INT is contributed by ATT construct followed by NB and SE.

6.10.6 Predictive Relevance, Q^2

Table 6.19 shows the results of Q^2 values for particular endogenous constructs in the model after a blindfolding procedure using omission distance D.=11. The table shows Q^2 for all endogenous constructs in this research are more than 0, and this indicates path model's predictive relevance for ATT, NB, SE and INT constructs in the research model.

Table 6.19 Q^2 Values

	SSO	SSE	Q^2 (=1-SSE/SSO)
ATT	2,416.00	2,038.86	0.156
INT	2,416.00	1,459.28	0.396
ISC	17,516.00	8,598.48	0.509
ISK	3,020.00	3,020.00	
ISKS	3,020.00	3,020.00	
MON	2,416.00	2,416.00	
NB	1,812.00	1,324.10	0.269
PCM	2,416.00	2,416.00	
RM	1,812.00	1,812.00	
SE	1,812.00	1,557.97	0.140
SETA	2,416.00	2,416.00	
TMC	2,416.00	2,416.00	

This also means exogenous constructs have predictive relevance for endogenous construct under consideration. This indicates that each path in the model from ISC towards ATT, NB and SE respectively as well as from ATT, NB and SE towards INT have predictive relevance.

6.10.7 Mediation Results and Analysis

This research also examined the mediation effects of three behavioral factors of ATT, NB and SE in the relationship between ISC and INT. Table 6.20 shows the results of indirect effect on the relationship between ISC and INT for each mediator of ATT, NB and SE after a bootstrapping procedure with 5000 sub-samples.

Table 6.20 Results of Indirect Relationships

Relation	Std Beta	Std Error	*t*-value	p-value	CI (LL)	CI (UL)
ISC -> ATT-> INT	0.254	0.026	9.846	p<0.001	0.203	0.304
ISC -> NB-> INT	0.288	0.029	10.304	p<0.001	0.232	0.344
ISC -> SE -> INT	0.151	0.023	6.469	p<0.001	0.107	0.198

In general, the results show all mediators have significant effect in the relationship between ISC and INT with t > 1.96 (two-tailed). Specifically, the indirect effect between ISC and INT mediated by NB is the strongest with $\beta = 0.288$ and *t*-value = 10.304, which is significant at $p < 0.001$. This is followed by the indirect effect between ISC and INT mediated by ATT, which is significant with $\beta = 0.254$ and *t*-value 9.846, at $p < 0.001$. These findings are consistent with Flores and Ekstedt (2016) who discovered ATT and NB mediate the relationship between ISC and INT but in different case of intention, which is the intention to resist to social engineering. This means ATT and NB are significant mediators that influencing the relationship between ISC and employees' intention towards improving security behavior and minimizing security threats. As for SE, the indirect effect between ISC and INT mediated by this construct is also significant with $\beta = 0.151$ and *t*-value = 6.469, at $p < 0.001$. Finally, Confidence Interval (CI) for all indirect relationships do not straddle a zero (Preacher & Hayes, 2008) which is also another indication that all relationships tested are significant.

6.11 Results of Hypotheses Testing

Table 6.21 shows the results of hypotheses testing for direct relationships of H1, H2, H3, H4, H5 and H6, whereas Table 6.22 shows the hypothesis testing of H7, H8 and H9 for indirect relationships (mediation). The tables show all hypotheses are supported by passing all assessment criteria. Based on results and analysis conducted, the following sub-sections conclude all the hypotheses for this research.

Table 6.21 Summary Results of Hypothesis Testing (H1 – H6)

Hypothesis	Relation	Std Beta	Std Error	*t*-value	p-value	f^2	LL	UL	VIF	R^2	Q^2	Result
H1	ISC -> ATT	0.427	0.032	13.426	p<0.001	0.223	0.371	0.478	1	0.182	0.156	Supported***
H2	ISC -> NB	0.550	0.033	16.849	p<0.001	0.435	0.496	0.602	1	0.303	0.269	Supported***
H3	ISC -> SE	0.394	0.037	10.731	p<0.001	0.183	0.331	0.453	1	0.155	0.140	Supported***
H4	ATT -> INT	0.429	0.045	9.565	p<0.001	0.239	0.354	0.503	1.395			Supported***
H5	NB -> INT	0.228	0.048	4.777	p<0.001	0.063	0.149	0.304	1.506	0.449	0.396	Supported***
H6	SE -> INT	0.195	0.033	5.832	p<0.001	0.060	0.140	0.250	1.152			Supported***

**p < 0.01; ***p<0.001

Table 6.22 Summary Results of Hypothesis Testing (H7 – H9)

Hypothesis	Relation	Std Beta	Std Error	*t*-value	p-value	LL	UL	Result
H7	ISC -> ATT -> INT	0.254	0.026	9.846	p<0.001	0.203	0.304	Supported***
H8	ISC -> NB-> INT	0.288	0.029	10.034	p<0.001	0.232	0.344	Supported***
H9	ISC -> SE -> INT	0.151	0.023	6.469	p<0.001	0.107	0.198	Supported***

**p < 0.01; ***p<0.001

6.11.1 The Influence of ISC towards Employee's Attitude, Normative Belief and Self-Efficacy

Hypothesis 1 (H1) states that ISC positively influences employee's Attitude towards compliance with ISP (ATT). The results of path coefficients obtained show ISC has strong significant relationship with ATT with $\beta = 0.427$ at *t*-value = 13.426 ($p < 0.001$). Therefore, H1 is supported.

Hypothesis 2 (H2) states that ISC positively influences employee's Normative Belief (NB) about ISP compliance. The results of path coefficients obtained show ISC has strong significant relationship with NB with $\beta = 0.550$ at *t*-value = 16.849 ($p < 0.001$). Therefore, H2 is supported.

Hypothesis 3 (H3) states that ISC positively influences employee's Self-Efficacy (SE) to comply with ISP. The results of path coefficients obtained show ISC has strong significant relationship with SE with $\beta = 0.394$ at *t*-value = 10.731 ($p < 0.001$). Therefore, H3 is supported.

Moreover, according to Table 6.21, Confidence Interval (CI) for each hypothesis 1, 2 and 3 does not contain zero and these additional criteria proved all hypotheses are supported.

6.11.2 The Influence of Attitude, Normative Belief and Self-Efficacy towards ISP Compliance Intention

Hypothesis 4 (H4) states that Attitude towards ISP compliance (ATT) positively influences employee's intention to comply with ISP (INT). The results of path coefficients obtained show ATT has strong significant relationship with INT with $\beta = 0.429$ at *t*-value = 9.565 ($p < 0.001$). Therefore, H4 is supported.

Hypothesis 5 (H5) states that Normative belief about ISP compliance (NB) positively influences employee's intention to comply with ISP (INT). The results of path coefficients obtained show NB has significant relationship with INT with $\beta = 0.228$ at *t*-value = 4.777 ($p < 0.001$). Therefore, H5 is supported.

Hypothesis 6 (H6) states that Self-Efficacy to comply with ISP (SE) positively influences employee's intention to comply with ISP (INT). The results of path

coefficients obtained show SE has significant relationship with INT with β = 0.195 at *t*-value = 5.832 (p < 0.001). Therefore, H6 is supported.

Moreover, according to Table 6.21, Confidence Interval (CI) for each hypothesis 4, 5 and 6 does not contain zero and these additional criteria proved all hypothesis are supported.

6.11.3 The Role of Attitude, Normative Belief and Self-Efficacy in Mediating the Relationship between ISC and Intention to Comply

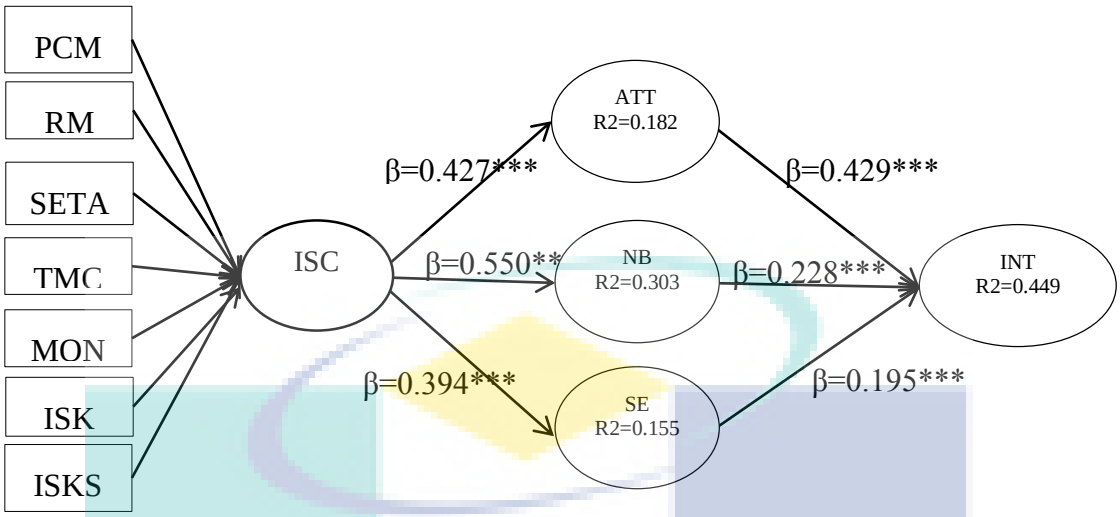
Hypothesis 7 (H7) states the relationship between ISC and intention to comply (INT) is mediated by Attitude towards ISP compliance intention (ATT). The results of bootstrapping procedure show the indirect relationship between ISC and INT is significant with β = 0.254 at *t*-value = 9.846 (p < 0.001). According to Table 6.22, Confidence Interval (CI) values also do not straddle a zero. This result reveal that ATT mediates the relationship between ISC and INT. Therefore, H7 is supported.

Hypothesis 8 (H8) states the relationship between ISC and intention to comply (INT) is mediated by Normative Belief about ISP compliance (NB). The results of bootstrapping procedure obtained show the indirect relationship between ISC and INT is significant with β = 0.288 at *t*-value = 10.034 (p < 0.001). According to Table 6.22, Confidence Interval (CI) values also do not straddle a zero. This result reveal that NB mediates the relationship between ISC and INT. Therefore, H8 is supported.

Hypothesis 9 (H9) states the relationship between ISC and intention to comply (INT) is mediated by Self-Efficacy to comply with ISP (SE). The results of bootstrapping procedure obtained shown the indirect relationship between ISC and INT is significant with β = 0.151 at *t*-value = 6.469 (p < 0.001). According to Table 6.22, Confidence Interval (CI) values also do not straddle a zero. This result reveal that SE mediates the relationship between ISC and INT. Therefore, H9 is supported.

6.11.4 Summary of Structural Model Assessments

Figure 6.9 shows the structural model with annotation of path coefficients (β) and portions of variance explained (R^2). It shows that all relationships hypothesized are significant at p < 0.001.



*p < 0.05; ** p < 0.01; *** p < 0.001 (one-tailed tests)

Figure 6.9 Structural Model Assessments

6.12 Discussion of the Findings

In general, the findings support general conceptual frameworks of this research. Seven dimensions of Procedural Countermeasures (PCM); Risk Management (RM); Security Education, Training and Awareness (SETA), Top Management Commitment (TMC), Monitoring (MON), Information Security Knowledge (ISK) and Information Security Knowledge Sharing (ISKS) are important and significant dimensions of ISC concept. This ISC concept has significantly influenced employees' behavior factors of Attitude (ATT), Normative Belief (NB) and Self-Efficacy (SE), and in turn has influenced their ISP compliance intention. The model produced in this study has high predictive accuracy, indicating strong explanatory power of the model. It is also more parsimony than other previous models that predict ISP compliance behavior from the perspective of ISC. The next sections discuss all the findings in details.

6.12.1 Information Security Culture Dimensions

Due to the inconsistency of dimensions used to represent ISC concept, the first objective (RO1) of this research is to formulate appropriate dimensions to represent ISC concept. By using the most widely accepted concepts in ISC literature, which are Organizational Culture (OC) by Schein (1999) and ISC framework by Van Niekerk and Von Solms (2006), seven dimensions were formulated to represent ISC concept in this

research, which answer Research Question 1 (RQ1). Next, to achieve Research Objective 2 (RO2), this ISC concept was integrated with the most significant behavioral theory in ISP compliance behavior literature, which is Theory of Planned Behavior (TPB) to form ISC model for ISP compliance behavior. This model answers Research Question 2 (RQ2).

Then, to achieve Research Objective 3 (RO3), Research Objective 4 (RO4) and Research Objective 5 (RO5), this dimension-based ISC model for ISP compliance behavior was tested. The results show the weights of all seven dimensions formulated are relevant and significant in contributing to ISC concept. This proves that seven dimensions formulated based on Organizational Culture (OC) by Schein (1999) and ISC conceptual framework by Van Niekerk and Von Solms (2006) are relevant and significant in representing the ISC concept of the study. Analysis on VIF also proves that each dimension represents the distinct aspect of ISC. These suggested that all the seven aspects are uniquely contributing to the concept of ISC that effectively influence employees' security behavior in the organization especially in Malaysian public university context. Thus, all seven aspects uniquely contribute to the forming of ISC concept as depicted in Figure 6.10. In addition, the order of dimensions based on their importance is determined and they are ISK, TMC, ISKS, SETA, MON, PCM and RM. Three dimensions including ISK, TMC and ISKS have the most relative contribution towards ISC. It is important to note that ISK is the top most among the three. These particular findings answered Research Question 3a (RQ3a) and Research Question 3b (RQ3b).

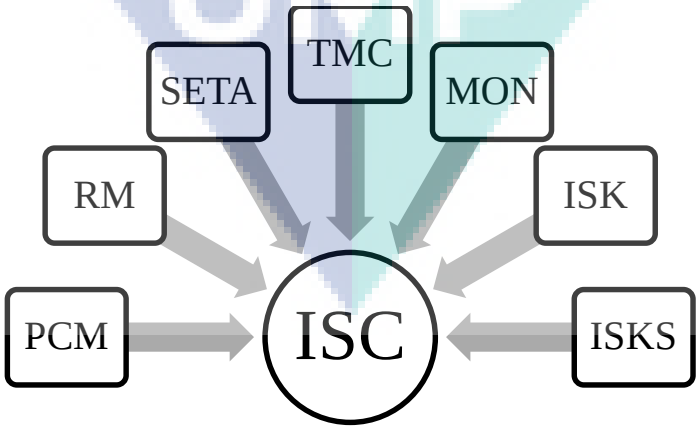


Figure 6.10 Dimensions of ISC concept

The aforementioned findings are consistent with D'Arcy and Greene (2014) who found three dimensions of Security Communications, Top Management Commitment and Monitoring are the significant dimensions of ISC concept. Nevertheless, findings of this study also prove that several other important dimensions significantly contribute to the concept such as ISK and ISKS dimensions. Even though, these dimensions were not involved in D'Arcy and Greene (2014) study, they are among the most relevant and significant dimensions in ISC concept. Another important dimension was not considered in D'Arcy and Greene (2014) is RM; and this research proves it is also a significant dimension of ISC. Since ISC is sub-culture of OC, the findings reveal those seven dimensions represent a comprehensive set of ISC component based on OC.

Furthermore, the dimensions produced in this research can be viewed from OC perspective particularly in terms of levels represented by particular dimensions. For example, dimensions of PCM and RM in this research were identified as artifacts level in OC concept. In contrast, dimensions in D'Arcy and Greene (2014) did not consider the levels in OC and there is combination of levels in one dimension. For example, dimensions of Security Communications in D'Arcy and Greene (2014) is a combination of two level of OC, which are Artifacts and Espoused Value.

ISC concept based on OC perspective is important since ISC is always related to OC and some studies argued that ISC is a subculture of OC. Furthermore, the classification of dimensions based on levels makes the planning and implementation of ISC strategies more practical and easier. For example, Van Niekerk and Von Solms (2010) have demonstrated various types of ISC based on strength and stability. Since Van Niekerk and Von Solms (2010) used levels (artifacts, espoused value, shared basic assumption, knowledge) to explain strength and stability in each type of ISC, the dimensions produced in this research assist academicians and practitioners to use and apply ISC concept more easily as they could directly use the dimensions instead of levels. The following sub-sections discuss each dimension in details based on its order of importance in contributing to ISC concept.

6.12.1.1 Information Security Knowledge

This research discovers that the most important dimension of ISC concept is Information Security Knowledge (ISK). Prior study by Van Niekerk and Von Solms

(2006, 2010) has argued that this aspect is essential in the context of ISC by adding the level of security knowledge into three existing levels of Schein's Organizational Culture (OC) in their ISC framework. According to Van Niekerk and Von Solms (2006, 2010), three levels of Schein's OC only form basic aspects of any organizational culture. The information security knowledge level must present in the case of ISC so that this level could provide adequate knowledge of information security on each level of existing OC. Without adequate knowledge of information security, those three culture levels do not have sufficient information pertaining to information security and are not be able to form the desired and stable ISC. This research confirms this argument by providing empirical findings, which clearly show ISK is the most important dimension of ISC concept.

In establishing a positive ISC to effectively influence employees' security behavior, an organization especially a public university must have dedicated unit/section/department responsible for information security. In the university, this unit is an IT department which comprises of experts or staff with adequate IT knowledge and skills. The staff must have adequate, appropriate and the most recent knowledge of information security so that they could successfully manage various information security issues. Adequate information security knowledge posed by this unit ensures the appropriateness of information security planning, implementation and audit in the organization. Furthermore, adequate ISK enables this unit to plan and organize suitable and effective information security programs to staff in improving their knowledge and skills regarding information security. The strength of this unit reflects the stability of information security management of the organization. The reason is the success or failure of information security in organization is determined by this unit in managing all information security aspects and issues. Therefore, the organization must ensure that they have strong IT unit so that they have adequate ISK for information security management.

6.12.1.2 Top Management Commitment

ISC is part of management efforts and top managers must champion this effort to show that information security is prioritized in the organization. Thus, the dimension of Top Management Commitment (TMC) has essential role in ISC and this research proves that this aspect is the second most important dimension of ISC concept. It is not

an easy task to establish ISC in the organization in order to attain meaningful support from employees throughout the organization. Top management should carefully plan and implement ISC strategies and show they are committed in this particular issue. The purpose is to gain employees' attention, trust and belief that this culture is necessary and relevant. As a result, they influence employees to follow the culture. Schein (1999) supported this as he claimed, "any prospective change in the current corporate culture requires, in essence, the unlearning of beliefs on the part of the employees and could result in a huge amount of anxiety and resistance to change from employees". As such, top managers should put strong commitment on ISC strategies to assist employees adapting to ISC.

In showing that information security is an important agenda in the organization, top management must clearly demonstrates that information security is one of the key values considered in establishing the vision, mission, objectives and goals of the organization. They must establish clear and comprehensive information security strategy understood by all employees. Additionally, they must support these strategies by allocating adequate budget and support to implement information security related matters. Consequently, employees should either directly or indirectly accept, trust and believe that top management is committed in ensuring information security in the organization. They should follow and give their commitment for information security which eventually becomes a culture among the employees.

6.12.1.3 Information Security Knowledge Sharing

The third important dimension of ISC concept in relation to employees' security behavior is Information Security Knowledge Sharing (ISKS). Generally, knowledge of information security is vital; however, sharing of this knowledge throughout the organization is also crucial to ensure it is received by those in need. This is consistent with Zakaria (2007) who suggested security knowledge needs to be externalized in order to be shared and learned by other employees. This activity ensures all employees get the required information and knowledge and eventually minimizes security incidents as well as overcomes any security breach that might occur or prevent them from happening in the first place.

The management should promote knowledge sharing activity by encouraging employees to share, participate and collaborate with each other in tasks involving information security such as email attachments, security updates, malware and any other new information technology software and hardware. It ensures the knowledge is transferred, disseminated and distributed so it is available to those requiring it (Hassan et al., 2013). As a result, all employees should work together in disseminating and sharing their knowledge of which finally it would become a norm and culture in the organization.

6.12.1.4 Security Education, Training and Awareness (SETA)

While information security knowledge is the top most important dimension of ISC concept, SETA programs are important tools in generating, promoting and disseminating information security knowledge and skills throughout the organization. Thus, dimension of SETA plays important role in forming ISC concept by providing meaningful supports for other ISC dimensions. Specifically, SETA is a comprehensive program designed by the management to realize information security planning and strategies. These programs ensure employees are aware and properly understand various information security aspects and their responsibilities towards information security in the organization. The employees are trained and educated on related information security issues especially the requirements and issues documented in the organizational ISP. They are taught and explained about the importance of information security and the consequences of information security violation.

As discussed in Section 6.12.1.1, adequate information security knowledge posed by the organization especially by IT Unit/Department helps them identify the appropriate knowledge and skills that should be posed by all employees and specific group of employees in the organization. This information then is used to plan and organize effective SETA program and campaign to their employees based on the time and requirements. They should be able to identify the frequency and type of SETA program to be conducted to the employees. This means that every employee will have adequate training, education and awareness programs so that they have adequate knowledge and skill of information security to work and behave securely in dealing with information security assets. Instead of having basic SETA program for knowledge and skills, the employees will have special and dedicated programs based on their needs

and requirements. Finally, these effective SETA becomes a value that espouses throughout the organization which in turn creates positive ISC in the organization.

6.12.1.5 Monitoring

Apart from top management commitment, belief and trust from the employees that their computer activities are always being monitored by the organization is crucial in forming positive ISC that effectively influences employees' security behavior. These assumptions make the employees to always be careful and aware when performing information and computing activities. As argued by Van Niekerk and Von Solms (2010), these shared tacit assumptions act as a kind of ''filter'', which affects how individuals carry out their normal day-to-day activities.

In ensuring this aspect, the organization must conduct monitoring mechanisms by performing periodic audits and reviews logs of employees' computing activities as well as periodic checks on unauthorized software tools and applications in employees' computer. These activities not only contribute to positive ISC, it also will gain attention and awareness from employees to believe that the employer monitors their computing activities. Consequently, these assumptions ensure the security behavior from employees and encouraging them to comply with the rules and policies established by the organization.

6.12.1.6 Procedural Countermeasures

This research confirms that Procedural Countermeasures (PCM) is one of significant dimensions for ISC concept. This also suggests that PCM is required in positive ISC establishment. As discussed in the formulation of this dimension in Section 3.3.1 (Chapter 3), the dimension involves guidelines, procedures and policies set up by the organizations to guide information security matters. PCM is an artifact which mostly is referred to ISPs, and must be established because it is the initial step to shape security culture in an organization (Chen et al. 2015). An organization must introduce and establish these security policies and they must be communicated throughout the organization. These policies act as guidelines and code of conducts to employees in dealing with information assets. Complying to these policies eventually becomes routine to the employees. ISP also is widely accepted in the literature as a common key factor of ISC.

From the context of OC level, this aspect represents artifacts that accessible to the employees and could be identified by the outsiders (Schein, 1999, p. 15). Most of the universities in Malaysia have published their ISP in their websites so that it can be accessible and identified by both insiders and outsiders. In this way, a well-designed ISP also represents a manifestation to a university that information security is a culture practised by the university.

6.12.1.7 Risk Management

The last important dimension of ISC concept and aspect that must exist in ISC establishment is Risk Management (RM). From the perspective of OC, it is also an ISC artifact alongside with PCM accessible to employees. The outsiders could identify RM as a unit of entity or process inside the organization that directly deals with risk mitigation. While PCM deals with procedural countermeasures, RM deals with technical countermeasures in terms of risk assessment and risk analysis. These risk management activities and processes would ensure the organization's information and systems are free from potential threats and breaches.

Information security risks such as threat of viruses, hackers or natural disasters need to be identified and controls need to be implemented by considering a cost benefit analysis (Veiga, 2008). Adequate controls on these risks ensure confidentiality, integrity and availability of information assets in the organization. In ensuring positive ISC, the organization must have adequate risk assessment and risk analysis plans appropriately implemented. Risk assessment is first fundamental step in gauging the level of information security risk in organization (ISO/IEC 13335-1, 2004). By applying security risk analysis and assessment, organizations and staff members are able to realize their security damages and create security aware culture for their security practices (Alnatheer, 2015).

6.12.2 The Influence of ISC towards Employees' Attitude, Normative Belief and Self-Efficacy

In general, this research supports the recommendation by experts and scholars that the establishment of positive ISC would guide employees' security behavior by providing empirical evidences on the relationship. More importantly, this research proposes an ISC model for ISP compliance behavior with clearer dimensions of ISC.

The ISC concept based on seven dimensions proposed was found significant in influencing employees' Attitude (ATT), Normative Belief (NB) and Self-Efficacy (SE) towards adhering to organization's ISP. These findings support hypothesis H1, H2 and H3, and answer Research Question 4a (RQ4a) as empirical evidences clearly show that there are strong significant relationships between ISC and these three behavioral factors. With these findings, Research Objective 4a (RO4a) is achieved.

Specifically, seven dimensions identified based on all levels of ISC and OC representing the aspects of positive ISC that would significantly influence employees' ATT, NB and SE towards ISP compliance. This means that organizations could establish ISC to promote these three behavior factors by implementing all seven dimensions discussed in Section 6.12.1. These findings are important since these three behavioral factors are widely proven in ISP compliance behavior literature as the most significant factors in influencing employees' ISP compliance intention.

Among three behavioral factors, the most influenced by the implementation of ISC in organization is NB followed by ATT and SE. Clearly, this research found that ISC has large effect towards NB. This is consistent with the findings by Flores and Ekstedt (2016) that found ISC has more influence on NB rather than ATT, but in different case of research objective. As discussed in Section 2.13.1 (Chapter 2), Flores and Ekstedt (2016) studied intention to resist social engineering, whereas this research focuses on ISP compliance intention. Nevertheless, this means ISC is effective in cultivating and influencing employees' norm towards safer behavior in the organizational context.

Apart from that, employee's NB about ISP compliance also has the most variance explained by ISC followed by ATT and SE. These findings suggest that in public university settings, ISC mostly influences employees' perceived social pressure pertaining to ISP compliance caused by behavioral expectations of such important referents as executives, colleagues, and managers. Then, this ISC is able to influence and improve employees' attitude towards adhering to ISP and perceived it as important, useful and beneficial to them. Finally, the ISC is able to influence and improve employees' personal skills, knowledge and competency towards fulfilling ISP requirements. Eventually, these behavioral factors is able to influence their intention to comply with ISP. While these findings on the relationship between ISC and three

behavioral factors of ATT, NB and SE are consistent with most of the theoretical findings in the literature (Alhogail et al., 2015; Mahfuth et al., 2017; Leanne Ngo et al., 2009; Tang et al., 2016), these findings also prove the relationships with clear seven dimensions of ISC concept. Therefore, instead of just confirming ISC influences employees' ISP compliance behavior, these findings also reveal the dimensions of a positive ISC that could effectively influence employees' security behavior.

6.12.3 The Influence of Employees' Attitude, Normative Belief and Self-Efficacy towards ISP Compliance Intention

Consistent with hypothesis H4, H5 and H6, this research discovers that three determinants of ISP compliance intention, which are Attitude (ATT), Normative Belief (NB) and Self-Efficacy (SE) have significant influence on employees' ISP compliance intention (INT). Besides being consistent with the literature that these three factors are the strongest predictors for ISP compliance intention, these findings also prove the resilience and reliability of TPB in predicting individual behavior in many contexts of social and organizational including ISC. From the context of ISC, the findings show that an employee's intention to comply with ISP is determined by his/her ATT, NB and SE as theorized by TPB. Thus, this research proves that these three behavioral factors play significant role in ensuring employees' ISP compliance. In short, it answers RQ4b and supports the theory.

This study also discovers that among three behavioral factors, attitude of employee towards adhering to ISP has the strongest influence towards his/her ISP compliance intention. This is consistent with findings in the literature such as by Kim et al. (2014); Sommestad, Karlzén, et al. (2014); Ifinedo (2014a); Ifinedo (2012); and Borena and Bélanger (2013), even though these particular studies examined these relationships in different types of organization. This finding also suggests organizational type does not influence the relationships between ATT, NB and SE with employees' ISP compliance intention. Furthermore, this fact is supported by previous studies of which control variable of organizational type has no significant effect on employee's ISP compliance intention.

Although it was shown that ISC has the strongest influence towards employee's NB rather than ATT and SE, in the case of intention to comply (INT), ATT has the most

influence towards INT compared to the influence of NB and SE towards INT. This particular finding is consistent with empirical findings in the literature (e.g. Ifinedo, 2012, 2014a; Kim et al., 2014; Kranz & Haeussinger, 2014; Sommestad, Karlzén, et al., 2014). This means that although ISC has mostly influenced an employee's normative belief on ISP compliance in the organization, in the case of intention to comply, an employee's attitude towards adhering to ISP has stronger influence towards his/her intention to adhere to ISP. This suggests that to ensure employees' compliance with ISP, the organization must ascertain their employees have positive attitude towards ISP compliance.

This research also found that in Malaysian public university settings, an employee's SE has less influence on his/her intention to comply with ISP (INT). Although the findings show that the relationship is significant, the effect is relatively small compared to ATT and NB. Generally this is consistent with the findings by Al-Omari et al. (2012); and Ifinedo (2012) who also discovered SE's least influential role compared to ATT and NB. The weaknesses of relationship between SE and INT were also found in Kranz and Haeussinger (2014), Ifinedo (2014a), Ifinedo (2012), Cox (2012), Al-Omari et al. (2012), Johnston and Warkentin (2010a) and Siponen et al. (2010). In fact, it is consistent with meta-analysis conducted by Cram et al. (2017a) who found SE has medium magnitude of effect size in relation to ISP compliance behavior compared to ATT and NB that have larger magnitude of effect sizes.

To certain extent, few studies found that SE is not significant in influencing INT such as in Kim et al. (2014); and Hovav and Putri (2016). This scenario suggests that SE is the weakest factor from the three main factors of TPB in this research area. These research findings have added more evidence in supporting this fact. This suggests that employees' knowledge, skill and ability to comply with ISP requirements may not matter as much as attitude and normative belief in the organization. Therefore, organization should give less attention on their employees' self-efficacy but focuses more on their employees' attitude and normative belief. This also means that organization especially public universities should not provide too much skills training; instead they should focus more on awareness programs. Nevertheless, considering that self-efficacy also has significant influence towards ISP compliance intention, all three factors are crucial in ensuring ISP compliance in Malaysian public university settings..

As depicted in Figure 6.11, the findings in this section and previous section have proved that ISC concept based on seven dimensions would positively influence employees' ISP compliance behavior. Besides that, additional analysis of Q^2 on the whole model reveals that the model has high predictive relevance. This means that the relationships proposed in the model are not only significant but also relevance in relating one construct to another. Furthermore, the model has high predictive accuracy especially in predicting employees' ISP compliance behavior. Therefore, these particular findings answer Research Question 4b (RQ4b) and achieve Research Objective 4b (RO4).

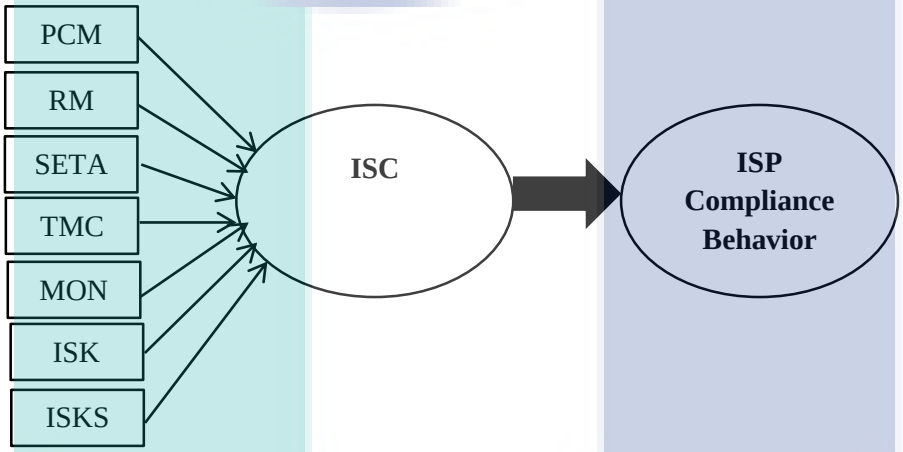


Figure 6.11 The Influence of ISC towards ISP Compliance Behavior

6.12.4 The Role of Attitude, Normative Belief and Self-Efficacy in Mediating the Relationship between ISC and ISP Compliance Intention

This research also examined the roles of ATT, NB and SE in mediating the relationships between ISC and INT as the last objective of this research. This examination reveals the existence and importance of these desired behavioral factors in the relationship between ISC and INT. The results support the notion that ATT, NB and SE mediate the relationship between ISC and INT. In general, the analysis shows that these three behavioral factors are significant in mediating the relationship between ISC and INT in Malaysian public university settings. These findings answer Research Question 5 (RQ5), achieve Research Objective 5 (RO5) and support Hypothesis H7, H8 and H9. This means that ATT, NB and SE are important in ensuring the effectiveness of ISC in influencing INT. These findings are consistent with Hu et al. (2012) who unearthed three main TPB constructs that mediate the relationship between OC and

INT. This suggests ISC is subculture of OC as the influence of ISC towards INT is also mediated by the same factors that mediate OC towards INT. These findings also justify the inclusion of these ATT, NB and SE factors in the model by proving that these three behavioral TPB constructs are actually intervening the relationship between ISC and employees' ISP compliance intention.

Among the three factors, NB has the most significant effect as mediator in the relationship followed by ATT with slightly the same strength as mediator effect. This means an employee's perceived social pressure caused by behavioral expectations of other employees about adhering to ISP is the most significant factor in ensuring the influence of ISC towards his/her ISP compliance intention. Thus, organizations such as public universities must ensure that these norms are adequate among their staff. At the same time, an employee's positive attitude towards complying to ISP also determines the influence of ISC towards his/her ISP compliance intention. Finally, an employee's personal skills, knowledge and competency about fulfilling ISP requirements are also important since these abilities assist ISC influence on INT. All in all, these three behavioral factors are required for establishing ISC that would effectively improve employees' ISP compliance intention. Therefore, to ensure that ISC influences employees' ISP compliance intention, they should have positive cognitive belief in terms of ATT, NB and SE in relation with ISP compliance.

6.13 Chapter Summary

This chapter presents, analyzes and discusses the findings of the research. It was discovered that all seven formulated dimensions are relevant and significant in contributing to ISC concept. Then, this ISC concept was found to be significant in influencing ISP compliance behavioral factors of ATT, NB and SE, which in turn was found significant in influencing ISP compliance intention (INT). These three behavioral factors are also significant in mediating the relationship between ISC and INT. The ISC model developed has high predictive accuracy and predictive relevance in predicting ISP compliance behavior. The next chapter concludes all these findings with the aims to re-examine each research question and research objective, to justify the contributions and implications, to recommend the possible future research and to identify limitations of this research.

CHAPTER 7

CONCLUSION

7.1 Introduction

This thesis focuses on the development and validation of ISC model based on seven formulated dimensions for ISP compliance behavior. Following the introduction of the research in Chapter 1, literature review was elaborated in Chapter 2 to understand the research problems, to determine the gaps and to identify the significant theory and concepts in ISC and ISP compliance behavior literature. Based on the findings from review in Chapter 2, the research model and related hypotheses were proposed in Chapter 3. Chapter 4 discusess and justifies the methodology employed to achieve the research objectives. Research instrument development was discussed in Chapter 5. It was followed by the quantitative model testing and the discussion of the findings in Chapter 6.

This chapter concludes all findings, addresses contributions and implications of the study as well as discusses the limitations and the possible future research directions. It contains seven sections. The next section discusses research objectives achievement followed by summary of research questions, research objectives, method and findings in section three. Meanwhile, the fourth section discusses theoretical, methodological and managerial contribution and implications of this doctoral research. Section five highlights the limitations of this research followed by suggestions for future research in section six. Section seven concludes all the findings of ISC model based on dimensions from the context of Organizational Culture and ISC. Finally, a brief summary is presented at the end of this chapter.

7.2 Research Objectives Achievement

Scholars and experts recommend practitioners to establish positive Information Security Culture (ISC) in guiding employees' security behavior in the organization. However, it remains unclear of what are the aspects should be implemented to establish positive ISC and what is the actual influence of ISC towards employees' ISP compliance behavior. Based on these research problems, the study thoroughly investigates the concept of ISC from more clear dimensions and examines its relation towards ISP compliance behavior to produce a dimension-based ISC model based for employee's ISP compliance behavior.

The research framework was proposed to validate ISC concept based on seven dimensions as well as to test nine hypotheses on the particular relationships between ISC and ISP compliance behavior in an attempt to answer research questions (RQs) of the study. In answering all the RQs, several objectives (ROs) were set to be achieved. The following sections discuss how ROs were attained.

7.2.1 Research Objective 1 (RO1)

The first objective of this research is to formulate appropriate dimensions to represent ISC concept. Since there are various approaches and theories adopted to conceptualize ISC in the literature, the most widely accepted concept in ISC, which are Organizational Culture (OC) by Schein (1999) and ISC conceptual framework by Van Niekerk and Von Solms (2006) were used as the underlying theories in the formulation of dimensions. These two concepts also represent theoretical frameworks and scope for the dimensions formulated in this study. The reason is many ISC factors and dimensions were produced in the literature and these two concepts justify the formulated dimensions. As discussed in Chapter 3 (Section 3.3 and Section 3.4), the mapping process from these two concepts produced seven comprehensive dimensions that cover all levels on both concepts and cover most ISC key factors available in the literature. The dimensions are Procedural Countermeasures (PCM), Risk Management (RM), Security Education Training and Awareness (SETA), Top Management Commitment (TMC), Monitoring (MON), Information Security Knowledge (ISK) and Information Security Knowledge Sharing (ISKS). This mapping was also supported by theoretical

and empirical findings from previous studies in the literature. These particular findings answer RQ1, and RO1 was achieved.

7.2.2 Research Objective 2 (RO2)

To achieve RO2, a conceptual model that links ISC concept based on formulated dimensions and ISP compliance behavior was developed and related hypotheses were proposed. The most significant theoretical framework in ISP compliance behavior literature, which is Theory of Planned Behavior (TPB) was adopted to form nomological core of the conceptual framework that links ISC with ISP compliance behavior. TPB main constructs of Attitude (ATT), Normative Belief (NB) as well Self-Efficacy (SE) were used to represent ISP compliance behavior factors. Meanwhile, Intention to Comply with ISP (INT) was used as the main dependent variable in this research. The model proposed the relationships between ISC concept based on seven dimensions and three constructs of ATT, NB and SE, as well as the relationships between ATT, NB and SE with INT. All these findings were discussed in Chapter 3 (Section 3.5) and with these findings, RO2 was achieved.

7.2.3 Research Objective 3 (RO3)

As to achieve RO3, this dimension-based ISC model for ISP compliance behavior was validated in Malaysian public universities settings. The multidimensional ISC concept then was tested and the results have shown that the weights of all seven dimensions formulated are relevant and significant in contributing to ISC concept. This proves that all seven dimensions formulated based on Organizational Culture (OC) by Schein (1999) and ISC conceptual framework by Van Niekerk and Von Solms (2006) are relevant to represent ISC concept. Analysis on VIF also proves that each dimension represents the distinct aspect of ISC, suggesting all seven dimensions uniquely contribute to the concept of ISC. Thus, in answering RQ3a, seven aspects of PCM, RM, SETA, TMC, MON, ISK and ISKS formulated based on widely accepted concepts of OC and ISC are found relevant and significant as a comprehensive set of dimensions for the ISC concept. As for RQ3b, the analysis reveals that ISK is the most important dimension in forming ISC concept compared to other dimensions. These particular findings were presented and discussed in Chapter 6 (Section 6.9 and Section 6.12.1). Thus, with these findings, RO3 was achieved.

7.2.4 Research Objective 4 (RO4)

The model validation shows ISC concept based on seven dimensions was found significant in influencing employee's Attitude (ATT), Normative Belief (NB) and Self-Efficacy (SE) towards adhering to organization's ISP. These findings answer the RQ4a with empirical evidences clearly show that there are strong significant relationships between ISC and these three behavioral factors.

As for RQ4b, the findings reveal that three determinants of ISP compliance intention (INT), which are ATT, NB and SE have significant influence on employee's INT. Overall, the model has acceptable quality in terms of predictive relevance and predictive accuracy. These particular findings were presented and discussed in Chapter 6 (Section 6.10.2 until Section 6.10.6, Section 6.12.2 and Section 6.12.3). Therefore, RO4 (a and b) was achieved.

7.2.5 Research Objective 5 (RO5)

RO5 was achieved by examining mediation effect of ATT, NB and SE in the relationship between ISC and INT. The findings reveal that all three behavioral factors have significant effect as a mediator on the relationship. This findings prove the importance of these three behavioral factors in ensuring the effectiveness of ISC in influencing ISP compliance intention in an organization. These findings were presented and discussed in Chapter 6 (Section 6.10.7 and Section 6.12.4). These findings answer RQ5.

7.3 Summary of Research Question (RQ), Research Objective (RO), Research Method and Findings

Table 7.1 summarizes the research questions, research objectives, methods and findings of this research. According to the table, each research question was answered with its specific findings using particular methods to achieve the associated research objective.

Table 7.1 Summary of Research Question, Research Objective, Method and Findings

Research Question (RQ)	Research Objective (RQ)	Method/Analysis	Findings
RQ1. What are the appropriate dimensions should be used to represent ISC based on Organizational concept?	RO1. To formulate ISC dimensions based on widely accepted concepts of Organizational Culture and Information Security Culture	• Mapping OC (Schein, 1999) and ISC framework (Van Niekerk and Von Solms, 2006) levels into ISC dimensions • Identifying all ISC key factors in literature to determine the comprehensiveness of dimensions produced	• Seven dimensions associated with all levels in OC and ISC were produced • Cover most ISC key factors in literature
RQ2. What is the model to address the relationship between ISC and ISP compliance behavior?	RO2. To develop a model of ISC based on new formulated dimensions for employee's ISP compliance behavior	• Using TPB and its main constructs of ATT, NB and SE to link ISC concept based on seven dimensions with employee's intention to comply with ISP • Developing and justifying hypotheses	• Conceptual framework of dimension-based ISC model for employee's ISP compliance behavior
RQ3. What is the relationship between the formulated dimensions and ISC concept? RQ3a. Are these dimensions relevant and significant in contributing to the underlying concept of ISC? RQ3b. Which dimension is the most important in forming the ISC concept	RO3. To validate the formulated dimensions in representing ISC conceptual model	• Survey • PLS SEM – the relationship of first-order and second-order construct • Outer weight - Relative contribution and its significance • VIF • Confidence Interval	• All seven dimensions are relevant and significant in contributing to the underlying concept of ISC • ISK is the most important • VIF values less than 5 • CI values did not straddle zero

Table 7.1 continued

Research Question (RQ)	Research Objective (RQ)	Method/Analysis	Findings
RQ4. What is the relationship between the ISC concept based on formulated dimensions with employees' ISP compliance behavior? RQ4a. What is the relationship between this ISC concept with employee's ATT, NB and SE towards ISP compliance behavior?	RO4. To validate ISC model for employee's ISP compliance behavior in Malaysian public universities RO4a. To examine the relationships between ISC concept with employee's Attitude, Normative Belief and Self-Efficacy	• Survey • PLS SEM – the relationship between ISC based on 7 formulated dimensions with ATT, NB and SE. • Path Coefficient • Effect Size • R^2 • Q^2	• ISC has significant relationship towards ATT, NB and SE • Effect size – ATT (Medium, NB (Large), SE (Medium) – Cohen (1988) • R^2 – ATT (Moderate), NB (Substantial), SE (Moderate) – Cohen (1988)
RQ4b. What is the relationship between these three behavioral factors and ISP compliance intention?	RO4b. To examine the relationships between employee's Attitude, Normative Belief and Self-Efficacy with ISP compliance intention	• Survey • PLS SEM – the relationships between ATT, NB and SE with INT. • Path Coefficient • Effect Size • R^2 • Q^2	• ATT, NB and SE has significant relationships towards INT • Effect size - ATT (Medium), NB (Small), SE (Small) – Cohen (1988) • R^2 –High (Hair et al., 2014)
RQ5. What are the roles of Attitude, Normative Belief and Self-Efficacy in mediating the relationship between ISC and ISP compliance intention?	RO5. To validate the roles of Attitude, Normative belief and Self-Efficacy in mediating the relationship between ISC and ISP compliance intention	• PLS SEM – the relationship between ISC and INT mediated by ATT, NB and SE. • Indirect Relationship • Confidence Interval	• Indirect relationships are significant • CI did not straddle zero • ATT, NB and SE mediate the relationship between ISC and INT. • ATT, NB and SE are important in the relationship between ISC and INT

7.4 Contributions

This research expands both literature of ISC and ISP compliance behavior in terms of theoretical, methodological and managerial contributions. The following sub-sections discuss the contributions in details.

7.4.1 Theoretical Contributions

This research provides theoretical contributions for ISC literature and information security behavior literature. First, the findings contribute to the content validity of ISC construct by identifying seven dimensions of Procedural Countermeasures, Risk Management, SETA, Top Management Commitment, Monitoring, Information Security Knowledge and Information Security Knowledge Sharing as dimensions of ISC concept. Although prior studies by D'Arcy and Greene (2014) have provided this knowledge by identifying three dimensions, this research provides more comprehensive dimensions based on the widely accepted concepts in ISC literature. This is crucial findings since Karlsson and Hedström (2014) claimed that more researches are needed to provide comprehensive view that guides and integrates all important factors in shaping or influencing the effectiveness of ISC. Moreover, there are calls for researches to provide comprehensive frameworks of ISC establishment (Tolah et al., 2017). Therefore, the findings provide insights on both issues by developing and validating a more comprehensive model based on seven reliable dimensions to facilitate ISC understanding and for ISC establishment in the organization.

Furthermore, since there is still no agreement on how to conceptualize ISC construct, this research provides new insight on ISC conceptualization by formulating seven ISC dimensions systematically mapped from widely accepted concepts in information security field, which are Organizational Culture by Schein (1999) and ISC conceptual framework by Van Niekerk and Von Solms (2006). Apart from enclosing all levels in these concepts and supported by theoretical and empirical findings from previous studies, the dimensions formulated also include the most important ISC key factors in the literature. Statistical results of model validation prove that all dimensions formulated are relevant and significant in forming the underlying concept of ISC. This

is a significant discovery indeed because holistic ISC concept based on comprehensive set of dimensions that could be referred to is still lacking in the literature.

Second, as this research discovers that Information Security Knowledge (ISK) is the most important dimension of ISC concept, it provides new important knowledge to ISC literature. Instead of typical PCM, MON and RM dimensions, the empirical findings prove that ISK is the most important dimension of ISC concept. Several previous studies highlighted the importance of ISK in conceptualizing the ISC such as those by Van Niekerk and Von Solms (2006, 2010) and recently by Mahfuth et al. (2017). However, the studies did not provide any empirical evidence to support the argument.

Furthermore, there is a lack of studies that empirically examines the relationship between dimensions with ISC concept especially involving ISK construct. Therefore, this research provides clear empirical findings on ISK being one of the important dimensions of ISC concept. The findings prove that adequate level of information security knowledge would provide desired knowledge for organizational culture in establishing a positive ISC. Additionally, this research also provides new insight on the conceptualization and operationalization of ISK construct with adequate construct reliability and validity.

Third, it is worth to note again that ISC depends on the types of organization (Ayyagari & Tyks, 2012; Dojkovski et al., 2007b; Kuusisto & Ilvonen, 2003; Lopes & Oliveira, 2014; Main et al., 2009; Williams, 2009b) and national culture (Connolly & Lang, 2013; Govender, Kritzinger, & Loock, 2016). This study provides significant contribution to ISC literature by providing specialized findings of ISC concept and model for Malaysian public university. The findings show specific detail of a positive ISC, particularly on the priority of each dimension for improving employees' security behavior in this sector.

Fourth, this research adds new knowledge on the influence of ISC towards ISP compliance behavior by providing more conclusive findings on the relationship. The findings prove that ISC based on the seven dimensions would significantly influence ISP compliance behavior among employees in the organization. While this finding expands ISC literature, it also contributes to ISP compliance behavior literature by

adding new insight on how to promote employees' security behavior. Furthermore, since this study focuses on sole effect of ISC towards employee's security behavior, the findings could represent the actual relationship between ISC and ISP compliance behavior.

Fifth, since this study investigates the relationship between ISC and ISP compliance behavior from the theoretical perspective of Theory of Planned Behavior (TPB), the findings provide in-depth understanding and richer knowledge on the relationship. It is consistent with Schein (2004) who suggested to study culture by building profound and more complex anthropological models. To date, to the best knowledge of the author, this is the first study that employed all three TPB main constructs of Attitude, Normative Belief and Self-Efficacy in the research model linking ISC and ISP compliance intention. This is also the first study that examines the effect of ISC based on particular dimensions towards these three behavioral factors as well as examines the relationships of these three factors towards ISP compliance intention in a research model. Therefore, the findings provide new knowledge on the influence of ISC towards these significant behavioral factors, and how these factors influence ISP compliance intention.

To date, to the best knowledge of the author, this is the first study that empirically shows that the effect of ISC on employees' ISP behavioral intention (INT) is actually mediated by ATT, NB and SE. This suggest that ISC may influence employees' cognitive beliefs of ATT, NB and SE, but does not directly lead to their behavioral intention. These findings refine the understanding of how ISC works in organizational settings in terms of its influence towards employees' security behavior. These behavioral factors of ATT, NB and SE do not only influence INT but also mediate the relationship between ISC and ISP compliance behavior. These findings also expand the applicability of TPB in bridging the relationship between ISC and ISP compliance intention.

All in all, the findings suggest that from the perspective of organizational culture, a positive ISC is determined by seven dimensions of PCM, RM, SETA, TMC, MON, ISK and ISKS. The stronger these dimensions or aspects are, the more positive ISC is in influencing employees' ISP compliance behavior in the organization.

7.4.2 Methodological Contributions

This research provides several methodological contributions in terms of conceptualizing, operationalizing and validating the research model particularly ISC concept and model. Firstly, to date, to the best knowledge of the author, this is the first study that formulates ISC dimensions by systematically mapping them from widely accepted concept of Organizational Culture (OC) by Schein (1999) and ISC conceptual framework by Van Niekerk and Von Solms (2006). The dimensions formulated not only relevant and significant in contributing to ISC concept but also cover all ISC key factors available in the literature. This means ISC conceptualization based on seven dimensions formulated using mapping process from OC and ISC concepts is valid and relevant. Moreover, the dimensions formulated are supported by theoretical and empirical evidences from the literature.

Second, ISC conceptualization and operationalization as a second-order reflective-formative multidimensional construct provides new knowledge on how to model and measure the ISC concept from more comprehensive view and approach. This adds new insight on how ISC concept should be modeled and validated in order to thoroughly examine this complex concept. Specifically, ISC concept is modeled as a formative higher-order construct formed by seven reflective ISC dimensions as the first-order constructs. ISC is a complex concept and has variety of dimensions; therefore, the approach used to model and validate ISC in this research was appropriate. Furthermore, the use of the latest approaches in PLS-SEM during model validation provide new insights by demonstrating more rigorous assessment to the ISC concept and model. This provides important contribution to ISC literature since there is a lack of validated approach in the study of ISC model in the literature (Fredrik Karlsson et al., 2015).

Third, this is the first study that investigates mediating effects of ATT, NB and SE in the relationship between ISC and ISP compliance intention (INT). The examination and analysis of mediation in this research is genuinely in the context of ISP compliance behavior by using intention to comply with ISP (INT) as main dependent variable. This study examines all main constructs of TPB, which are ATT, NB and SE as mediators in the relationship between ISC and ISP compliance intention. Compare to previous studies, this study employs the latest approaches of mediation testing and analysis proposed by Memon, Cheah, Ramayah, Ting, and Chuah (2018); and Zhao et

al. (2010) which prove to be more accurate compared to Baron and Kenny (1986) approach. All in all, these aspects are significant to produce more convincing and conclusive findings to the literature.

Fourth, from the perspective of ISP compliance behavior literature, study by D 'Arcy et al. (2009) is the only study that examines ISP compliance behavior based on the sole effect of ISC. However, as discussed in Section 2.13.1 (Chapter 2), the ISC concept used in their study did not cover most of ISC dimensions that available in the literature. Apart from that, other previous studies did not use ISC as sole predictors for ISP compliance behavior in the research model. Therefore, the model produced could not represent a solid ISC model for predicting ISP compliance behavior. In contrast, the model produced in this research focuses on the sole effect of ISC concept towards ISP compliance behavior. This means that the model predicts ISP compliance behavior purely from one antecedent or variable under focus of the study. This research proves that the model produced is more focused, parsimonious and has high predictive accuracy. This also means that the model could be used as effective reference for understanding, improving and cultivating a positive ISC in the organization.

7.4.3 Managerial Contributions

Empirical findings of the study on the relationships between seven formulated dimensions with ISC concept which significantly influence employees' information security behavior provides clear guidelines in terms of aspects and best practices required in establishing a positive ISC for influencing employees' security behavior in organization especially in Malaysian public universities. Since ISC depends on national culture and type of organization, these findings are crucial for educational sector also as it is one of the most impacted sectors for security incidents and breaches caused mainly by employees' behavior. It is important to note that the sample population used in this study is sufficient to generalize the findings to this sector particularly to Malaysian Public Universities. Moreover, high predictive accuracy of the model also suggests that this model could be effectively used as reference in ISC cultivation to improve security behavior in the organization. Therefore, the model could be directly applied to all public universities, other higher education provider or any other sectors and organizations that have similar settings with public universities.

The model provides organizations with a means to implement effective Information Security Management (ISM) approach, which includes the provision of guides and implementation controls in understanding the importance of aspects involved in establishing ISC. The findings in terms of seven significant aspects of ISC complement Information Security Management System (ISMS) standards and guidelines such as ISO/IEC 27001. While ISMS standards provides general guidelines in managing information security technology, the ISC model could be used as specific guidelines of ISC cultivation and assessment to improve employees' security behavior in the organization. Managing technological aspects do not guarantee a total solution of information security. In fact, most incidents are caused by employees' behavior, not the technology. Therefore, instead of adopting the standards alone, the practitioners could directly adopt the ISC model as an effective guideline to establish ISC that would significantly improve security behavior of their employees. This model is the answer for practitioners who are seeking for guidelines in terms of aspects that should be used to implement a positive ISC in mitigating information security risk in the organization.

While seven formulated dimensions are significant aspects of a positive ISC, clearly, the most important aspects are Information Security Knowledge (ISK) and Top Management Commitment (TMC) as well as Information Security Knowledge Sharing (ISKS). The organizations including HEIs must have adequate up-to-date security knowledge by strengthening Information Technology Unit/Department or ISM entity that is responsible for Information and Communications Technology (ICT) management in the organization. Adequate experts and person-in-charge who are ready to adopt and adapt new knowledge and technology of ICT should be provided. Top management including policy makers must support any information security initiative and show their commitment for its implementation. Finally, the top management together with ISM must promote information security importance among employees by encouraging and providing them with conducive facilities and environment to share information security knowledge.

Generally, PCM, SETA, MON and RM are the common aspects in ISMS (ISO/IEC 27001). Interestingly, this research reveals that the top most important dimensions of ISC are ISK and ISKS, which are not given an appropriate focus in ISMS. This indicates that adopting ISMS does not mean positive ISC will be

established in the organization; therefore, it does not guarantee employees' security behavior. These crucial findings justify why even with the adoption of ISMS standards, security incidents still occur. The reason is those standards are for general information security and do not focus on employees' security behavior. Most successful attacks were caused by insiders' behavior which fail to follow ISP in dealing with information assets. ISC guides employees' behavior and to a certain extent promotes human firewall (Zakaria, 2013). Technology and appliances act as firewall that is always there and protecting as it should be, but security attacks are not caused by its weaknesses. It is caused by human who lacks "firewall" within themselves. This is consistent with several studies indicating information security can not be achieved by technological issues alone as it is also associated with personal issues such as employees' behavior who actually operate these systems (Connolly, Lang, Gathegi, & Tygar, 2017). Therefore, the ISC model produced in this research could assist practitioners in establishing total solution of information security in the organization.

The findings on the importance of ISK also suggest that most information security problems are caused by the inappropriateness of information security knowledge in planning, implementing and reviewing information security programs and strategies in the organization. As argued by Van Niekerk and Von Solms (2006, 2010) this knowledge is important as they determine on what to be protected, why need to be protected and how to protect each asset and aspect of information security throughout organization. This is also the answer as to why despite adopting ISMS standards, there are always problems of non-compliance to this standard such as outdated procedures, inadequate security applications and other issues of inadequate technical countermeasures. All these issues obviously caused by the lack of information security knowledge which limits practitioners' ability to establish adequate information security in the organization. Therefore, alongside with the adoption of ISMS, organization especially Malaysian public universities must establish ISC based on the proposed seven aspects with extra effort on information security knowledge. ISMS focuses more on the implementation of physical, policy and technical measures to mitigate anticipatory threats. On the other hand, ISC could be used to reduce security problems by improving employees' security behavior. While ISMS focuses on establishing comprehensive set of controls comprises of best practices in information security, the seven aspects of ISC dimensions formulated and validated in this research can be

guidelines of comprehensive aspects for establishing ISC that effectively influence employees' ISP compliance behavior.

This research demonstrates that three behavioral factors of ATT, NB and SE do not only have significant influence towards employees' ISP compliance intention, but also play significant role for ISC's effectiveness in influencing employees' ISP compliance intention. Thus, practitioners must bring their employees' attitude, normative belief and self-efficacy at acceptable level so that security behavior can be inculcated among the employees in the organization. Interestingly, this research has empirically proven that this could be achieved by establishing positive ISC strategies based on the seven aspects proposed. In other words, since the model is integrated with these three significant behavioral factors, it could be used to aid in directing employees' behavior towards the desired information security behavior.

7.4.4 Underlying Theory and Basis for ISC Audit System

Results on the relationships between seven dimensions with ISC construct that significantly influence employees' security behavior could be used as the basis and underlying structure in developing ISC audit system. ISC audit system is Decision Support System that is capable of assessing ISC level in the organization. This audit system is crucial for regular planning, maintaining and improving ISC. By using this system, information security practitioners could evaluate ISC current level, provide status of current ISC aspects and suggest recommendations to improve the level of current ISC. The values and order of importance for each dimension in forming significant relationship with ISC in the study could be used as cut-off value and prioritizing aspects in determining the desired ISC in the organization. The system could also be used to audit and predict security behavior in order to achieve the desired employees' security behavior. Since most incidents are caused by insiders behavior who fail to comply to ISP, the system is crucial particularly for organizations to improve their information security.

There are only few ISC audit systems available and most of these systems did not employ a proven approach or basis in determining cut-off values and priority for each information security aspects assessed. Hence, no indication on what is the actual desired value for each aspect and which aspect is more important than the other. They

just assumed that these values are the cut-off that need to be achieved without strong justification from empirical findings. Therefore, the practitioners are not able to apply correct information in evaluating ISC aspects to improve their employees' security behavior.

7.5 Limitations of Study

This research has some limitations. First, since the formulation is based on OC by Schein (1999) and ISC conceptual model by Van Niekerk and Von Solms (2006), the dimensions formulated only cover the levels in those two concepts. The dimensions formulated are in terms of organizational efforts only. This means other non-organizational efforts, aspects and factors that are not directly related to the concepts of OC and ISC were not considered for the study. It includes regulatory requirements such as Data Protection Act, Protection of Personal Information Act or other regulatory requirements pertaining to data protection and information security (Da Veiga & Martins, 2015a) as well as organizational behavior factors such as Job Satisfaction and Personality Traits (Tolah et al., 2017). Although this research found that no significant difference on ISC influence towards ISP compliance intention among job types, there might be some differences in terms of ISC for each of profession in public university settings as Ramachandran et al. (2008) revealed that there are significant differences in belief and values on group of profession in organization. This research also assumes that all employees share the same general attributes.

Second, the model was only tested in Malaysian Public Universities. Therefore, the model is directly applicable to HEIs and other organizations that have similar setting to public university. However, on wider perspective, since this model especially the dimensions were formulated based on universal concept of ISC and OC, the findings should be applicable to all types of organizations as they have similar concept of ISC and OC. Nevertheless, some differences in terms of strength and priority of the dimensions among different types of organizations may be noticed.

Third, this research only used one stage approach for data collection. This means data for Independent Variables (IV) and Dependent Variables (DV) were collected at the same time from the respondents. Although the analysis and results show that CMV was not an issue in this research, the use of two stage approach by separating collection

of independent and dependent variables will reduce more the likelihood of common method effects (Podsakoff et al., 2003). However, it is difficult to obtain for more than 400 responses. It is already difficult to get the respondents volunteer to participate in the study in the first place, it is even more difficult to maintain the same respondent to answer another part of questionnaire for the second time. In terms of generalization of findings, it is also very difficult to obtain respondents that could represent the population of all public universities in Malaysia.

Finally, the behavioral factors employed in this research were based on theoretical framework of TPB only. This means other behavioral constructs from other theories such as Protection Motivation Theory (PMT) and General Deterrence Theory (GDT) were not involved in this study. Recent meta-analysis by Cram et al. (2017) found that factors from PMT and GDT such as Response Efficacy, Respond Cost, Threat Severity and Detection Certainty have medium effect size towards ISP compliance behavior alongside with TPB construct of SE. Although these factors did not have large effect like ATT and NB of TPB, there is a possibility that the ISC also influences employees' behavioral factors from PMT and GDT, which in turn influence their ISP compliance intention.

7.6 Future Works

Since the model was validated in Malaysian public universities settings only, it is suggested that future works to replicate this study for other industries and sectors. This will expand the findings to wider perspective especially in determining ISC concept for other types of organization. The findings will provide crucial knowledge as it will reveal ISC concept based on dimensions for all types of organization. While this knowledge could be used to cultivate ISC for these type of organizations, the findings will contribute more to the literature by providing complete view of ISC concept based on dimension for all type of organization.

In order to get more reliable findings, future study should employ two stage approach in data collection. As discussed in Section 7.5, this approach will reduce CMV effects in the collected data. However, a comprehensive effort is required to conduct this two-stage approach. Adequate budget and time, high commitment from employees to participate and full support from employers are required to realize this approach.

From the context of ISP compliance behavior, future works could also be conducted by considering other behavioral factors from other behavioral theories such as PMT and GDT. Therefore, in-depth knowledge could be developed on how ISC will affect these particular behavioral factors. Da Veiga and Martins (2015b) argued that ISC is related to culture of protecting the information. Since PMT is a theory that is related to protection behavior and motivation, the examination of ISC relationship towards PMT behavioral factors would provide knowledge on how ISC influences employees' threat appraisal and coping appraisal in relation to protecting the information assets in the organization. As for GDT, the use its factor in the research model could provide useful findings on how ISC influences employees' behavior in the opposite direction, which is incompliance behavior. Thus, it will complement this research by revealing two types of behavior influenced by ISC.

7.7 ISC Model based on Organizational Culture and ISC Concepts

Based on this research findings, it was found that ISC is a subculture of Organizational Culture (OC). As OC would influence employees' behavior in an organization, ISC also has influence information security behavior to comply with ISP in the organization. OC concept (Schein, 1999) has three levels of artifacts, espoused values and basic assumptions. ISC as a subculture of OC required adequate information secuty knowledge as the forth level to ensure a stable ISC in the organization (Van Niekerk & Von Solms, 2006). Seven dimensions of PCM, RM, SETA, TMC, MON, ISK and ISKS based on these two concepts were found significant and important in establishing a positive ISC that would influence employees' ISP compliance behavior in the organization particularly in Malaysian public universities.

In addition, the main behavioral factors of Theory of Planned Behavior (TPB), which are Attitude (ATT), Normative Belief (NB) and Self-Efficacy (SE) play significant influence that ensure the establishment of ISC will improve the employees' intention to comply with ISP (INT). This is another prove that ISC is a subculture of OC as the literature show that the same behavioral factors were significant in the relationship between OC and INT.

7.8 Summary

This thesis presents a development and validation of ISC model based on seven comprehensive dimensions for employee's security behavior in the organization. The ISC dimensions were formulated from widely accepted concepts in ISC literature, which are Organizational Culture (Schein, 1999) and ISC conceptual framework (Van Niekerk & Von Solms, 2006). The model was integrated with the most significant theory in ISP compliance behavior, which is TPB in order to investigate the influence of ISC towards employee's information security behavior. The model was tested in Malaysian public universities setting. The findings show that all seven formulated dimensions are relevant and significant in contributing towards ISC concept, which in turn has significantly influenced employee's ISP compliance behavior. The model has high predictive accuracy compared to previous models especially in predicting employees' ISP compliance behavior based on the sole effect of ISC. While confirming scholars' and experts' recommendation to establish ISC for guiding security behavior, the findings also reveal that ISK is the most important aspect of positive ISC. Furthermore, this research also found that ATT, NB and SE are significant in mediating the relationship between ISC and ISP compliance intention. With all these findings, all the research objectives were achieved and all research questions were answered.

Thus, the findings indicate that establishing ISC based on seven aspects of PCM, RM, SETA, TMC, MON, ISK and ISKS is an effective strategy in guiding employees' security behavior in the organization. While all dimensions are significant, ISK was found to be the most important dimension of a positive ISC. This research provides an effective solution of ISC cultivation and assessment in managing employees' security behavior in the organization. Due to the fact that ISC dimensions were formulated based on general concept of OC and ISC, the model is also applicable as basic reference model to all types of organization. All in all, the findings provide crucial knowledge and effective model for institutionalization of information security in the organization especially in Malaysian HEIs.

REFERENCES

Abraham, S. (2011). Information security behavior: Factors and research directions. *17th Americas Conference on Information Systems 2011, AMCIS 2011*, *5*, 4050–4062.

Aguinis, H., Edwards, J. R., & Bradley, K. J. (2017). Improving Our Understanding of Moderation and Mediation in Strategic Management Research. *Organizational Research Methods*, *20*(4), 665–685.

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

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *32*(4), 665–683.

Ajzen, I. (2005). Attitudes, Personality, and Behavior - Icek Ajzen - Google Books. New York, NY: Open University Press. Albrechtsen, (2nd ed.).

Ajzen, I., & Madden, T. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology*, *474*, 453–474.

Al-Mayahi, I., & Mansoor, S. P. (2013). Information security culture assessment: Case study. In *Third International Conference on Information Science and Technology (ICIST)* (pp. 789–792).

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013). Information Security Policy Compliance: An Empirical Study of Ethical Ideology. *2013 46th Hawaii International Conference on System Sciences*, 3018–3027.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Information Security Policy Compliance: The Role of Information Security Awareness. In *Eighteenth Americas Conference on Information Systems, Seattle, Washington* (pp. 1–10).

Al Hogail, A., & Mirza, A. (2015). Organizational Information Security Culture Assessment. *International Conference on Security and Management*, 286–292.

Alfawaz, S. M. (2011). *Information security management: A case study of an information security culture*. Queensland University of Technology.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A behaviour compliance conceptual framework. *Conferences in Research and Practice in Information Technology Series*, *105*, 47–55.

Alharbi, N. (2017). *The Role of Security and Its Antecedents in E-Government Adoption*. Plymouth University.

Alhogail, A. (2015a). Cultivating and Assessing Organizational Information Security Culture, an Empirical Study, *9*(7), 163–178. http://doi.org/10.14257/ijsia.2015.9.7.15

Alhogail, A. (2015b). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*(August 2015), 567–575. http://doi.org/10.1016/j.chb.2015.03.054

Alhogail, A., & Mirza, A. (2014a). A proposal of an organizational information security culture framework. *Proceedings of International Conference on Information, Communication Technology and System (ICTS) 2014*, 243–250. http://doi.org/10.1109/ICTS.2014.7010591

Alhogail, A., & Mirza, A. (2014b). Information Security Culture: A Definition and a Literature review. In *Computer Applications and Information Systems (WCCCAIS)* (pp. 1–7). http://doi.org/10.1109/WCCAIS.2014.6916579

Alhogail, A., Mirza, A., & Saad, H. B. (2015). A Comprehensive Human Factor Framework for Information Security in Organizations. *Journal of Theoretical and Applied Information Technology*, *78*(2), 201–211.

Ali Memon, M., Ting, H., Ramayah, T., Chuah, F., & Cheah, J.-H. (2017). A Review of The Methodological Misconceptions and Guidelines Related to The Application of Structural Equation Modeling: A Malaysian Scenario. *Journal of Applied Structural Equation Modeling*, *1*(1), i–xiii.

Alkalbani, A., Deng, H., & Kam, B. (2015). Organisational Security Culture and Information Security Compliance For E-Government Development: The Moderating Effect of Social Pressure. In *Pacific Asia Conference on Information System (PACIS 2015)*.

Alnatheer, M. A. (2012). *Understanding and Measuring Information Security Culture in Developing Countries : Case of Saudi Arabia*. Queensland University of Technology.

Alnatheer, M. A. (2014). A Conceptual Model to Understand Information Security Culture. *International Journal of Social Science and Humanity*, *4*(2), 104–107. http://doi.org/10.7763/IJSSH.2014.V4.327

Alnatheer, M. A. (2015). Information Security Culture Critical Success Factors. In *2015 12th International Conference on Information Technology - New Generations* (pp. 731–735). http://doi.org/10.1109/ITNG.2015.124

Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding And Measuring Information Security Culture. In *Pacific Asia Conference on Information Systems (PACIS)* (pp. 1–15).

Alnatheer, M., & Nelson, K. (2009). Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. *Australian Information Security Management Conference*, (December), 6–17.

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613–643. http://doi.org/10.1016/j.arth.2009.05.009

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411–423. http://doi.org/10.1037/0033-2909.103.3.411

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers and Security*, *39*(PART B), 396–405. http://doi.org/10.1016/j.cose.2013.09.004

Aurigemma, S., & Mattson, T. (2014). Do it OR ELSE ! Exploring the Effectiveness of Deterrence on Employee Compliance with Information Security Policies. *Amcis 2014*, 1–12.

Aurigemma, S., & Mattson, T. (2015). The Role of Social Status and Controllability on Employee Intent to Follow Organizational Information Security Requirements. In *2015 48th Hawaii International Conference on System Sciences* (pp. 3527–3536). IEEE. http://doi.org/10.1109/HICSS.2015.424

Aurigemma, S., & Panko, R. (2011). A composite framework for behavioral compliance with information security policies. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3248–3257. http://doi.org/10.1109/HICSS.2012.49

Ayyagari, R., & Tyks, J. (2012). Disaster at a University: A Case Study in Information Security. *Journal of Information Technology Education: Innovations in Practice*, *11*, 85–96.

Aziz, N. S., & Kamaludin, A. (2014). Assessing website usability attributes using Partial Least Squares. In- ternational. *International Journal of Information and Electronics Engineering*, *4*(2), 137–144.

Baggett, W. O. (2003). Creating a culture of security. *The Internal Auditor*, *60*(3), 37–41. http://doi.org/10.1353/pla.2001.0074

Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing Construct Validity in Organizational Research. *Administrative Science Quarterly*, *36*(3), 421–458. http://doi.org/10.2307/2393203

Bagozzi, R., & Yi, Y. (1988). On the Evaluation of Structural Equation Models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94. http://doi.org/10.1177/009207038801600107

Baker, W., Goudie, M., Hutton, A., Hylender, C. D., Niemantsverdriet, J., Novak, C., & Ostertag, D. (2010). *Verizon 2010 Data Breach Investigations Report*. *Trends*. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Verizon+Data+Breach+Investigations+Report#2

Bakry, S. H. (2003). Development of security policies for private networks. *International Journal of Network Management*, *13*(3), 203–210. http://doi.org/10.1002/nem.472

Bandura, A. (1977). Self efficacy: Toward a unifing theory of behavioral change. *Psychological Review*, *84*(2), 191–215.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers and Security*, *39*(PART B), 145–159. http://doi.org/10.1016/j.cose.2013.05.006

Baron, R. M., & Kenny, D. A. (1986). The Moderator-Mediator Variable Distinction in Social Psychological Research. Conceptual, Strategic, and Statistical Considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173–1182. http://doi.org/10.1037/0022-3514.51.6.1173

Bauer, S., & Bernroider, E. W. N. (2017). From Information Security Awareness to Reasoned Compliant Action. *ACM SIGMIS Database: The DATA BASE for Advances in Information Systems*, *48*(3), 44–68. http://doi.org/10.1145/3130515.3130519

Beck, C. T., Bernal, H., & Froman, R. D. (2003). Methods to document semantic equivalence of a translated scale. *Research in Nursing & Health*, *26*(1), 64–73. http://doi.org/10.1002/nur.10066

Becker, G. S. (1968). *Crime and Punishment: An Economic Approach*. *Journal of Political Economy* (Vol. 76). http://doi.org/10.1086/259394

Becker, J.-M., Klein, K., & Wetzels, M. (2012). Hierarchical Latent Variable Models in PLS-SEM: Guidelines for Using Reflective-Formative Type Models. *Long Range Planning*, *45*(5–6), 359–394. http://doi.org/10.1016/j.lrp.2012.10.001

Becker, T. E. (2005). Potential problems in the statistical control of variables in organizational research: A qualitative analysis with recommendations. *Organizational Research Methods*, *8*, 274–289.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information and Management*, *54*(7), 887–901. http://doi.org/10.1016/j.im.2017.01.003

Berg, B. L. (2001). *Qualitative research methods for the social sciences*. Boston, MA: Allyn and Bacon.

Berita Harian. (2016). PressReader.com - Connecting People Through News. Retrieved January 17, 2017, from https://www.pressreader.com/

Bernerth, J. B., & Aguinis, H. (2016). A critical review and best-practice recommendations for control variable usage. *Personnel Psychology*, *69*, 229–283.

Borena, B. ., & Bélanger, F. . (2013). Religiosity and information security policy compliance. In *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime* (Vol. 4, pp. 2848–2855).

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in Information Systems Research: A State-of-the-Art Assessment. *MIS Quarterly*, *25*(1), 1. http://doi.org/10.2307/3250956

Boujettif, M., & Wang, Y. W. Y. (2010). Constructivist Approach to Information Security Awareness in the Middle East. *Broadband Wireless Computing Communication and Applications BWCCA 2010 International Conference on*. http://doi.org/10.1109/BWCCA.2010.70

Bozic, G. (2012). The role of a stress model in the development of information security culture. In *Proceedings of the 35th International Convention MIPRO, May 2012* (pp. 1555–1559).

Breaugh, J. A. (2006). Rethinking the control of nuisance variables in theory testing. *Journal of Business and Psychology*, *20*, 429–443.

Brewer, M. B. (2000). Research design and issues of validity. In *Handbook of Research Methods in Social and Personality Psychology* (pp. 3–16).

Brislin, R. W. (1970). Back-Translation for Cross-Cultural Research. *Journal of Cross-Cultural Psychology*, *1*(3), 185–216. http://doi.org/10.1177/135910457000100301

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009a). Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. In *Proceedings of the International Conference on Computational Science and Engineering, Vancouver*.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009b). Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance. *AMCIS 2009 Proceedings*, *419*, 1–9.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010a). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523–548. http://doi.org/10.1093/bja/aeq366

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010b). Quality and Fairness of an Information Security Policy as Antecedents of Employees' Security Engagement in the Workplace: An Empirical Investigation. *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, 1–7. http://doi.org/10.1109/HICSS.2010.312

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2011). Information security policy compliance : the role of fairness , commitment , and cost beliefs. *MCIS 2011 Proceedings*.

Cain, M. K., Zhang, Z., & Yuan, K.-H. (2016). Univariate and multivariate skewness and kurtosis for measuring nonnormality: Prevalence, influence and estimation. *Behavior Research Methods*. http://doi.org/10.3758/s13428-016-0814-1

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*, *56*(2), 81–105.

Cárdenas-Solano, L.-J., Martínez-Ardila, H., & Becerra-Ardila, L.-E. (2016). Gestión de seguridad de la información: revisión bibliográfica/ Information security management: A bibliographic review. *El Profesional de La Información*, *25*(6), 931–948. http://doi.org/10.3145/epi.2016.nov.10

Cardoso, M. G. M. S., Laureano, R. D., & Serrão, C. (2017). Cybersecurity culture in Portuguese organizations : an exploratory analysis. In *12th Iberian Conference on Information Systems and Technologies (CISTI)*.

Casper, W. J., & Harris, C. M. (2008). Work-life benefits and organizational attachment: Self-interest utility and signaling theory models. *Journal of Vocational Behavior*, *72*(1), 95–109. http://doi.org/10.1016/j.jvb.2007.10.015

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM*, *47*(7), 87–92. http://doi.org/10.1145/1005817.1005828

Champman, D. W., & Carter, J. F. (1979). Translation procedures for the cross cultural use of measurement instruments. *Educational Evaluation and Policy Analysis*, *1*, 71–76.

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*. http://doi.org/10.2307/3151312

Chang, S.-J., van Witteloostuijn, A., & Eden, L. (2010). From the Editors: Common method variance in international business research. *Journal of International Business Studies*, *41*(2), 178–184.

Chang, S. E., Lin, C.-S. S., Ho, C. B., Knapp, K. J., Marshall, T. E., Rainer, R. K., & Lin, C.-S. S. (2007). *Exploring organizational culture for information security management*. *Industrial Management and Data Systems* (Vol. 107). http://doi.org/10.1108/02635570710734316

Chen, Y. A. N., Ramamurthy, K. R. A. M., & Wen, K. (2015). Impacts of Comprehensive Information Security Programs on Information Security Culture. *Journal of Computer Information Systems*, *55*(3), 11–19.

Chen, Y., Ramamurthy, K. R., & Wen, K. (2013). Organizations ' Information Security Policy Compliance : Stick or Carrot Approach ? *Journal of Management Information Systems*, *29*(3), 157–188. http://doi.org/10.2753/MIS0742-1222290305

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*, 447–459. http://doi.org/10.1016/j.cose.2013.09.009

Chia, P. A., Maynard, S. B., & Ruighaver, A. . (2002a). Exploring Organisational Security Culture: Developing a comprehensive research model. In *Sixth Pacific Asia Conference on Information Systems, Tokyo, Japan* (pp. 1–11).

Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2002b). Understanding Organisational Security Culture. In *Sixth Pacific Asia Conference on Information Systems* (pp. 335–365).

Chin, W. W. (2010). How to Write Up and Report PLS Analyses. In *Handbook of Partial Least Squares* (pp. 655–690). http://doi.org/10.1007/978-3-540-32827-8_29

Chin, W. W., Thatcher, J. B., & Wright, R. T. (2012). Assessing Common Method Bias: Problems with the ULMC Technique. *MIS Quarterly*, *36*(3), 1003-A11. http://doi.org/10.1287/isre.1070.0123

Ciampa, M. D. (2012). *Security+ guide to network security fundamentals*. Course Technology, Cengage Learning.

CNN tech. (2017). Massive ransomware attack hits 99 countries - May. 12, 2017. Retrieved May 14, 2017, from http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences. Journal of the American Statistical Association 2nd (334).

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155–159. http://doi.org/10.1037/0033-2909.112.1.155

Cohen, J., & Cohen, P. (1983). *Applied multiple regression/correlation analysis for the bahavioral sciences* (2nd ed.). Hillsdale,NJ: Erlbaum.

Collis, J., & Hussey, R. (2003). *Business research: A practical guide for undergraduate and postgraduate students*. Palgrave macmillan.

Connolly, L., & Lang, M. (2013). Information Systems Security : The Role of Cultural Aspects in Organizational Settings. *Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy*, 1–15.

Connolly, L., Lang, M., & Tygar, D. (2014). Managing Employee Security Behaviour in Organisations: The Role of Cultural Factors and Individual Values. In *IFIP Advances in Information and Com- munication Technology* (pp. 417–430). http://doi.org/10.1007/978-3-642-55415-5_35

Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour A qualitative study. *Information and Computer Security*, *25*(2), 118–136.

Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, *28*(5), 1849–1858.

Cram, W. A., Proudfoot, J. G., & Arcy, J. D. (2017). Seeing the forest and the trees : A meta-analysis of information security policy compliance literature. *Proceedings of the 50th Hawaii International Conference on System Sciences*, 4051–4060.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2012). Future Directions for Behavioral Information Security Research. *Computers & Security*, *32*, 90–101. http://doi.org/10.1016/j.cose.2012.09.010

Cyber Security Malaysia. (2017). *Cybersecurity Malaysia Issues Alert on "Wannacry Ransomware."* Retrieved from http://www.cybersecurity.my/data/content_files/44/1674.pdf

CyberSecurity Malaysia. (2015). Cyber security trends & strategy for business (digital ?), (June).

D'Arcy, J., & Greene, G. (2009). The Multifaceted Nature of Security Culture and Its Influence on End User Behavior. In *IFIP TC 8 International Workshop on Information Systems Security Research* (pp. 145–157). in Proceedings of IFIP TC8 International Workshop on Information Systems Security Research, Cape Town, pp. 145-157.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474–489. http://doi.org/10.1108/IMCS-08-2013-0057

D'Arcy, J., & Herath, T. (2011). A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings. *European Journal of Information Systems*, *20*(6), 643–658. http://doi.org/10.1057/ejis.2011.23

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. http://doi.org/10.1287/isre.1070.0160

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study. *Information & Computer Security*, *24*(2), 139–151.

Da Veiga, A., & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information Systems Management*, *24*(May), 361–372. http://doi.org/10.1080/10580530701586136

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers and Security*, *29*(2), 196–207. http://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A., & Martins, N. (2015a). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162–176. http://doi.org/10.1016/j.cose.2014.12.006

Da Veiga, A., & Martins, N. (2015b). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, *31*(2), 243–256. http://doi.org/10.1016/j.clsr.2015.01.005

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72–94. http://doi.org/10.1016/j.cose.2017.05.002

Degirmenci, K., Guhr, N., & Breitner, M. H. (2013). Mobile Applications and Access to Personal Information: A Discussion of Users' Privacy Concerns. In *Proceedings of the International Conference on Information Systems* (pp. 1–21).

Detert, J. R., Schroeder, R. G., & Mauriel, J. J. (2000). A framework improvement for linking culture and in initiatives organization. *Academy of Management Review*, *25*(4), 850–863. http://doi.org/10.5465/AMR.2000.3707740

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers and Security*, *20*(2), 165–172. http://doi.org/10.1016/S0167-4048(01)00209-7

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting Information Security Culture : An organizational transformation case study. *Computers & Security*, *56*, 63–69. http://doi.org/10.1016/j.cose.2015.10.001

Dojkovski, S., Lichtenstein, S., & Warren, M. (2007a). Developing Information Security Culture in Small and Medium Size Enterprises: Australian Case Studies. In *Proceedings of the 6th European Conference on Information Warfare and Security* (pp. 55–65).

Dojkovski, S., Lichtenstein, S., & Warren, M. (2007b). Fostering information security culture in small and medium size enterprises: an interpretive study in Australia. In *Proceedings of the Fifteenth European Conference on Information Systems* (pp. 1560–1571).

Dojkovski, S., Lichtenstein, S., & Warren, M. (2007c). Institutionalising information security culture in Australian SMEs : Framework and key issues. In *International Symposium on Human Aspects of Information Security & Assurance* (pp. 10–24).

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2006). Challenges in Fostering an Information Security Culture in Australian Small and Medium Sized Enterprises. In *proceedings of the 5th European conference on Information Warfare and Security* (pp. 31–40).

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2010). Enabling information security culture: influences and challenges for Australian SMEs. In *21st Australasian Conference on Information Systems* (p. 61).

Dojkovski, S., Warren, M., & Lichtenstein, S. (2005). Information security culture in small and medium sized enterprises: a socio-cultural framework. In *Protecting the Australian homeland : conference proceedings of [the] 6th Australian Information Warfare & Security Conference* (p. 263). Deakin University, School of Information Systems.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers and Security*, *26*(1), 36–43. http://doi.org/10.1016/j.cose.2006.10.006

Duarte, P., & Amaro, S. (2018). Methods for modellingreflective-formative second order constructs in PLS: An application to online travel shopping. *Journal of Hospitality and Tourism Technology*. http://doi.org/10.1108/JHTT-09-2017-0092

Dugo, T. M. (2007). The Insider Threat to Organisational Information Security: A Structural Model and Empirical Test, 109.

Eagly, A. H., & Chaiken, S. (1993). The Nature of Attitudes. *Attitude Formation and Change*, 1–21.

Economist, T. (2014). Cyber-security - White hats to the rescue. Retrieved from www.economist.com/news/ business/21596984-law-abiding-hackers-are-helping-businesses-fight- bad-guys-white-hats-rescue

Edwards, J. R. (2001). Multidimensional Constructs in Organizational Behavior Research: An Integrative Analytical Framework. *Organizational Research Methods*, *4*(2), 144–192. http://doi.org/10.1177/109442810142004

Fagade, T., & Tryfonas, T. (2017). Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks. In *4th International Conference on Human Aspects of Information Security, Privacy, and Trust, HAS 2016* (Vol. 9750, pp. 128–139). http://doi.org/10.1007/978-3-319-58460-7

Fan, W., & Yan, Z. (2010). Factors affecting response rates of the web survey: A systematic review. *Computers in Human Behavior*, *26*(2), 132–139. http://doi.org/10.1016/J.CHB.2009.10.015

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. (2009). Statistical power analyses using G * Power 3 . 1 : *Behavior Research Methods*, *41*(4), 1149–1160. http://doi.org/10.3758/BRM.41.4.1149

Fischer, D. G., & Fick, C. (1993). Fischer, D. G. & Fick, C. Measuring Social Desirability: Short Forms of the Marlowe-Crowne Social Desirability Scale. Educ. Psychol. Meas. 53, 417–424 (1993).Measuring Social Desirability: Short Forms of the Marlowe-Crowne Social Desirability Scale. *Educational and Psychological Measurement*, *53*(2), 417–424.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior, An Introduction to Theory and Research*. *Belief, Attitude, Intention, and Behavior, An Introduction to Theory and Research*. http://doi.org/10.1016/B978-0-12-375000-6.00041-0

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26–44. http://doi.org/10.1016/j.cose.2016.01.004

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*. http://doi.org/10.2307/3151312

Frederick Van Niekerk, J. (2005). *Establishing an Information Security Culture in Organizations: An Outcomes Based Education Approach*. Nelson Mandela Metropolitan University.

Furnell, S., & Clarke, N. (2005). Organizational security culture: Embedding security awareness, education, and training. *Proceedings of the 4th World Conference on Information Security Education*, *11*(Dti), 67–74.

Furnell, S., & Clarke, N. (2012). Power to the people? the evolving recognition of human aspects of security. *Computers and Security*, *31*(8), 983–988. http://doi.org/10.1016/j.cose.2012.08.004

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly*, 51–90. http://doi.org/10.1017/CBO9781107415324.004

Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). Structural Equation Modeling and Regression : Guidelines for Research Practice. *Communications of the Association for Information Systems*, *4*(7), 1–77. http://doi.org/10.1.1.25.781

Glaspie, H. W., & Karwowski, W. (2018). Human Factors in Information Security Culture: A Literature Review. In *Advances in Intelligent Systems and Computing* (Vol. 593, pp. 269–280). http://doi.org/10.1007/978-3-319-60585-2

Govender, S., Kritzinger, E., & Loock, M. (2016). The Influence of National Culture on Information Security Culture. *Conference Proceedings*, 978–1. http://doi.org/10.1109/ISTAFRICA.2016.7530607

Greig, A., Renaud, K., & Flowerday, S. (2015). An Ethnographic Study to Assess the Enactment of Information Security Culture in a Retail Store, 61–66.

Guldenmund, F. . (2000). The nature of safety culture: a review of theory and research. *Safety Science*, *34*(1–3), 215–257. http://doi.org/10.1016/S0925-7535(00)00014-X

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information and Management*, *49*(6), 320–326. http://doi.org/10.1016/j.im.2012.08.001

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, *28*(2), 203–236. http://doi.org/10.2753/MIS0742-1222280208

Habermas, J. (1984). *The Theory of Communicative Action, Volume 1: Reason and the Rationalization of Society, translated by Thomas McCarthy*. Beacon Press, Boston.

Habermas, J. (1989). *The Theory of Communicative Action, Volume 2: Lifeworld and System: A Critique of Functionalist Reason, translated by Thomas McCarty*. Beacon Press, Boston.

Haeussinger, F. J., & Kranz, J. J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. In *ICIS2013* (pp. 1–16).

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (1998). *Multivariate Data Analysis. Prentice-Hall, Inc* (Vol. 1). http://doi.org/10.1038/259433b0

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Long Range Planning* (Vol. 46). http://doi.org/10.1016/j.lrp.2013.01.002

Hair, J. F. J., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2013). *A primer on partial least squares structural equation modeling (PLS-SEM). Long Range Planning* (1st ed., Vol. 46).

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *The Journal of Marketing Theory and Practice*, *19*(2), 139–152. http://doi.org/10.2753/MTP1069-6679190202

Hair, J. F., Sarsted, M., Ringle, C. M., & Guderga, S. P. (2018). *Advanced Issues in Partial Least Squares Structural Equation Modeling*. SAGE Publications, Inc.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications.

Hall, E. T. (1959). The silent language. In *The Silent Language* (pp. 73–76). http://doi.org/10.1007/s13398-014-0173-7.2

Hall, E. T. (1976). Beyond culture. *Contemporary Sociology*. http://doi.org/10.2307/2064404

Hamid, H., & Zeki, A. M. (2014). Users' awareness of and perception on information security issues: A case study of kulliyyah of ICT postgraduate students. *Proceedings - 3rd International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2014*, 139–144. http://doi.org/10.1109/ACSAT.2014.31

Han, J. Y., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers and Security*, *66*, 52–65. http://doi.org/10.1016/j.cose.2016.12.016

Hanus, B., & Wu, Y. A. (2016). Impact of Users??? Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), 2–16. http://doi.org/10.1080/10580530.2015.1117842

Hassan, N. H., & Ismail, Z. (2012). A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment. *Procedia - Social and Behavioral Sciences*, *65*(ICIBSoS), 1007–1012. http://doi.org/10.1016/j.sbspro.2012.11.234

Hassan, N. H., & Ismail, Z. (2016). Information Security Culture in Healthcare Informatics: A Preliminary Investigation. *Journal of Theoretical and Applied Information Technology*, *88*(2), 202–209.

Hassan, N. H., Ismail, Z., & Maarop, N. (2013). A conceptual model for knowledge sharing towards information security culture in healthcare organization. *2013 International Conference on Research and Innovation in Information Systems (ICRIIS), 2013*, 516–520. http://doi.org/10.1109/ICRIIS.2013.6716762

Hassan, N. H., Ismail, Z., & Maarop, N. (2014). Understanding Relationship Between Security Culture and Knowledge Management. *Knowledge Management in Organizations Lecture Notes in Business Information Processing*. http://doi.org/10.1007/978-3-319-08618-7_38

Hassan, N. H., Ismail, Z., & Maarop, N. (2015). Information Security Culture: A Systematic Literature Review, (205), 456–463.

Hassan, N. H., Maarop, N., Ismail, Z., & Abidin, W. Z. (2017). Information Security Culture in Health Informatics Environment : A Qualitative Approach. In *Conference on Research and Innovation in Information Systems (ICRIIS)*. Retrieved from http://ieeexplore.ieee.org.ezproxy.ump.edu.my/stamp/stamp.jsp?arnumber=8002450

Helokunnas, T., & Kuusisto, R. (2003). Information security culture in a value net. *IEMC '03 Proceedings. Managing Technologically Driven Organizations: The Human Side of Innovation and Change*, 190–194. http://doi.org/10.1109/IEMC.2003.1252258

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. http://doi.org/10.1007/s11747-014-0403-8

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. http://doi.org/10.1016/j.dss.2009.02.005

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. Retrieved from http://www.palgrave-journals.com/doifinder/10.1057/ejis.2009.6

Hina, S., & Dominic, D. D. (2016). Information Security Policies : Investigation of Compliance in Universities. In *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)* (pp. 1–6). IEEE. http://doi.org/10.1109/ICCOINS.2016.7783277

Hina, S., & Dominic, D. D. (2017). Need for Information Security Policies Compliance: A Perspective in Higher Education. In *IEEE* (pp. 1–6).

Hofstede, G. H. (2001). Culture's Consequences, Second Edition: Comparing Values, Behaviors, Institutions and Organizations Across Nations. In *Edn, Sage Publications, Inc, Thousand Oaks* (pp. 924–931). http://doi.org/10.1177/0022022110388567

Hofstede, G., Neuijen, B., & Ohayv, D. D. (1990). Measuring organizational cultures: a qualitative and quantitative study across twenty cases. *Administrative Science Quarterly*, *35*(2), 286–316.

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. http://doi.org/10.1016/j.im.2011.12.005

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, *32*, 35–49. http://doi.org/10.1016/j.pmcj.2016.06.007

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, *43*(4), 615–660. http://doi.org/10.1111/j.1540-5915.2012.00361.x

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54. http://doi.org/10.1145/1953122.1953142

Huczynski, A., & Buchanan, D. A. (2007). *Organizational behaviour: an introductory text*. *Organizational behaviour: an introductory text*.

Hulland, J. (1999). Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies. *Strategic Management Journal*, *20*(2), 195–204. http://doi.org/10.1002/(SICI)1097-0266(199902)20:2<195::AID-SMJ13>3.0.CO;2-7

Humaidi, N., & Balakrishnan, V. (2013). Exploratory Factor Analysis of User's Compliance Behaviour towards Health Information System's Security. *Journal of Health & Medical Informatics*, *4*(2), 2–9. http://doi.org/10.4172/2157-7420.1000123

Humaidi, N., & Balakrishnan, V. (2015). Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness. *International Journal of Information and Education Technology*, *5*(4), 311–318. http://doi.org/10.7763/IJIET.2015.V5.522

I-WAYS. (2003). *OECD Promotes Culture of Information Security*. *Digest of Electronic Commerce Policy and Regulation* (Vol. 26). IOS Press.

IBM Security. (2015). IBM 2015 Cyber Security Intelligence Index. *IBM Security Managing Security Services*, 24. Retrieved from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03073USEN&attachment=SEW03073USEN.PDF

Ifinedo, P. (2009). Information technology security management concerns in global financial services institutions. *Information Management & Computer Security*, *17*(5), 372–387. http://doi.org/10.1108/09685220911006678

Ifinedo, P. (2011). An exploratory study of the relationships between selected contextual factors and information security concerns in global financial services institutions. *Journal of Information Security and Privacy*, *7*(1), 25–49.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83–95. http://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014a). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79. http://doi.org/10.1016/j.im.2013.10.001

Ifinedo, P. (2014b). The Effects of National Culture on The Assessment of Information Security Threats and Controls in Financial Services Industry. *International Journal of Electronic Business Management*, *12*(2), 75–89.

Ifinedo, P. (2016). Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines? *Information Systems Management*, *33*(1), 30–41. http://doi.org/10.1080/10580530.2015.1117868

International Organization for Standardization. (2017). *ISO/IEC 27001 Information security management*. Retrieved from https://www.iso.org/isoiec-27001-information-security.html

ISF, I. S. F. (2000). Information Security Culture A Preliminary Investigation. *United Kingdom: ISF*.

Ismail, Z., Masrom, M., Sidek, Z., & Hamzah, D. (2010). Framework to Manage Information Security for Malaysian Academic Environment. *Journal of Information Assurance & Cybersecurity*, *2010*, 1–16. http://doi.org/10.5171/2010.305412

ISO/IEC 13335-1. (2004). Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management. Retrieved from https://webstore.iec.ch/preview/info_isoiec13335-1%7Bed1.0%7Den.pdf

Jakobsen, M., & Jensen, R. (2015). Common method bias in public management studies. *International Public Management Journal*, *18*(1), 3–30.

Järvinen, P. (2000). Research Questions Guiding Selection of an Appropriate Research Method. In *Proceedings of European Conference on Information Systems* (pp. 124–131).

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. *Journal of Consumer Research*, *30*(2), 199–218. http://doi.org/10.1086/376806

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security and Privacy*, *5*(3), 16–24. http://doi.org/10.1109/MSP.2007.59

Johnson, R. E., Rosen, C. C., Chang, C. H. D., Djurdjevic, E., & Taing, M. U. (2012). Recommendations for improving the construct clarity of higher-order multidimensional constructs. *Human Resource Management Review*. http://doi.org/10.1016/j.hrmr.2011.11.006

Johnston, A. C., & Warkentin, M. (2010a). Fear Appeals and Information Security Behaviors: An Empirical Study, *34*(3), 549–566.

Johnston, A. C., & Warkentin, M. (2010b). The influence of perceived source credibility on end user attitudes and intentions to comply with recommended IT actions. *Journal of Organizational and End User Computing*, *22*(3), 1–21. http://doi.org/10.4018/joeuc.2010070101

Kajtazi, M., & Bulgurcu, B. (2013). Information Security Policy Compliance : An Empirical Study on Escalation of Commitment. In *Nineteenth Americas Conference on Information Systems, Chicago, Illinois* (Vol. 3, pp. 2011–2020).

Karlsson, F., Astrom, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. *Information and Computer Security*, *23*(3), 246–285. http://doi.org/http://dx.doi.org/10.1108/ICS-05-2014-0033

Karlsson, F., & Hedström, K. (2014). End User Development and Information Security Culture. *Human Aspects of Information Security, Privacy, and Trust*. http://doi.org/10.4018/joeuc.2010101901

Kathryn, P., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, *66*, 40–51.

Kim, M. T., & Han., H. R. (2004). Cultural considerations in research instrument development. In Instruments for clinical health care research. In M. F.- Stromborg & S. J. Olsen (Eds.), *In Instruments for clinical health care research, ed* (ed, pp. 73–81). Boston: Jones & Bartlett.

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *TheScientificWorldJournal*, *2014*, 463870. http://doi.org/10.1155/2014/463870

Kline, R. B. (2005). *Principles and practice of structural equation modeling* (2nd ed.). New York: The Guilford Press. http://doi.org/10.1038/156278a0

Kline, R. B. (2011). *Principles and practice of structural equation modeling* (3rd ed.). The Guilford Press.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, *14*(1), 24–36. http://doi.org/10.1108/09685220610648355

Koh, K., Ruighaver, A., Maynard, S., & Ahmad, A. (2005). Security Governance : Its Impact on Security Culture. In *Proceedings of The third Australian Information Security Management Conference* (pp. 1–12).

Kolkowska, E. (2011). Security Subcultures in an Organization - Exploring Value Conflicts.

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non- compliance: Devising a Value-Based Compliance analysis method. *Journal of Strategic Information Systems*, *26*(2017), 39–57. http://doi.org/10.1016/j.jsis.2016.08.005

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*(5), 597–607. http://doi.org/10.1016/j.im.2003.08.001

KPT. (2016). *Dasar Keselamatan ICT Kementerian Pendidikan Tinggi*.

Kraemer, S., & Carayon, P. (2005). Computer and Information Security Culture: Findings from two Studies. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *49*, 1483–1488. http://doi.org/10.1177/154193120504901605

Kranz, J. J., & Haeussinger, F. J. (2014). Why Deterrence is not Enough: The Role of Endogenous Motivations on Employees' Information Security Behavior. *International Conference on Information Systems*, (October), 1–14.

Kuusisto, R., Nyberg, K., & Virtanen, T. (2004). Unite Security Culture May a unified security culture be plausible ? In *Proc. of the 3rd European Conference on Information Welfare and Security* (pp. 221–236).

Kuusisto, T., & Ilvonen, I. (2003). Information Security Culture in Small and Medium Size Enterprises. *Frontiers of E-Business Research*, 431–439.

Law, K. S., & Wong, C.-S. (1999). Multidimensional Constructs in Structural Equation Analysis: An Illustration Using the Job Perception and Job Satisfaction Constructs. *Journal of Management*, *25*(2), 143–160. http://doi.org/10.1016/S0149-2063(99)80007-5

Law, K. S., Wong, C.-S., & Mobley, W. H. (1998). Toward a taxonomy of constructs multidimensional. *Academy of Management Review*, *23*(4), 741–755.

Lebek, B., Guhr, N., & Breitner, M. H. (2014). Transformational Leadership and Employees' Information Security Performance: The Mediating Role of Motivation and Climate. *Icis*, 1–22.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. http://doi.org/10.1108/MRR-04-2013-0085

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. http://doi.org/10.1016/j.cose.2016.02.004

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of {SMB} executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(S2), 177–187. http://doi.org/10.1057/ejis.2009.11

Leonard, L. N. K., & Cronan, T. P. (2011). Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences. *Journal of the Association for Information Systems*, *1*(12), 1–31.

Li, H., Sarathy, R., & Zhang, J. (2010). Understanding Compliance with Internet Use Policy: An Integrative Model Based on Command- and-Control and Self-Regulatory Approaches. In *International Conference on Information Systems* (p. Paper 181).

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.

Lim, J. J. S., Ahmad, A., Chang, S., & Maynard, S. B. (2010). Embedding Information Security Culture Emerging Concerns and Challenges. In *Pacis 2010* (pp. 463–474).

Lim, J. S., Chang, S., Maynard, S. B., & Ahmad, A. (2009). Exploring the Relationship between Organizational Culture and Information Security Culture. In *7th Australian Information Security Management Conference* (pp. 88–97).

Limayem, M., & Hirt, S. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems*, *4*, 65–95.

Lohmöller, J.-B. (1989). *Latent Variable Path Modeling with Partial Least Squares*. *Physica-Verlag, Heidelberg*. http://doi.org/10.1007/978-3-642-52512-4_5

Lopes, I., & Oliveira, P. (2014). Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises. *New Perspectives in Information Systems and ...*, *1*(275), 277–286. http://doi.org/10.1007/978-3-319-05951-8

MacKenzie, S. B., Podsakoff, P. M., & Jarvis, C. B. (2005). The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. *Journal of Applied Psychology*. http://doi.org/10.1037/0021-9010.90.4.710

Mackenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques. *MIS Quarterly*, *35*(2), 293–334.

Magklaras, G., & Furnell, S. (2004). The Insider Misuse Threat Survey: Investigating IT misuse from legitimate users. In *International Information Warfare Conference, Perth, Australia*.

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1–6). http://doi.org/10.1109/ICRIIS.2017.8002442

Main, E., Ky, F., Dixie, W. D., Al-Hamdani, W. A., & Dixie, W. D. (2009). Information security policy in small education organization. *2009 Information Security Curriculum Development Conference on - InfoSecCD '09*, 72. http://doi.org/10.1145/1940976.1940991

Malcolmson, J. (2009). What is security culture? Does it differ in content from general organisational culture? *Proceedings - International Carnahan Conference on Security Technology*, 361–366. http://doi.org/10.1109/CCST.2009.5335511

MAMPU. (2010). *Dasar Keselamatan ICT Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU) Jabatan Perdana Menteri*. *Garis Panduan*. Retrieved from http://www.mampu.gov.my/documents/10228/3486670/DKICT_53.pdf/acaad8e2-b905-43b5-b4f3-465faf69790d

Martins, A. (2001). *Information Security Culture Survey*. *Rand Afrikaans University*.

Martins, A., & Eloff, J. (2002). Information Security Culture. *Security in the Information Society*, *86*(April), 203–214. http://doi.org/10.1007/978-0-387-35586-3_16

Martins, N., & Da Veiga, A. (2014a). Information Security Culture : A Comparative Analysis of Four Assessments. *European Conference on Information Management & Evaluation*, 49–58.

Martins, N., & Da Veiga, A. (2014b). The Value of Using a Validated Information Security Culture Assessment Instrument. In *Proceedings of the 8th European Conference on Information Management and Evaluation, ECIME 2014* (pp. 146–154).

Martins, N., & Da Veiga, A. (2015a). An Information Security Culture Model Validated with Structural Equation Modelling, (Haisa), 11–21.

Martins, N., & Da Veiga, A. (2015b). Factorial Invariance of an Information Security Culture Assessment Instrument for Multinational Organisations with Operations across Data Protection Jurisdictions. *Journal of Governance and Regulation*, *4*(4), 47–58. http://doi.org/10.22495/jgr

Masrek, M. N. (2017). Assessing Information Security Culture : The Case of Malaysia Public Organization. *Proc. of 2017 4th Int. Conf. on Information Tech., Computer, and Electrical Engineering (ICITACEE), Oct 18-19, 2017, Semarang, Indonesia Assessing*, 5386.

Masrek, M. N., Harun, Q. N., & Zaini, M. K. (2018). The Development of an Information Security Culture Scale for the Malaysian Public Organization. *International Journal of Mechanical Engineering and Technology*, *9*(July), 1255–1267.

Mcintosh, B. (2011). *An ethnographic investigation of the assimilation of new organizational members into an information security culture*. Nova Southeastern University.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334–359. http://doi.org/10.1287/isre.13.3.334.81

Mcllwraith, A. (2006). *Information security and employee behaviour : how to reduce risk through employee education, training and awareness*. Gower Publishing Company, Burlington.

Memon, M. A., Cheah, J.-H., Ramayah, T., Ting, H., & Chuah, F. (2018). Mediation Analysis : Issues and Recommendations. *Journal of Applied Structural Equation Modeling*, *2*(1), 1–9.

Merhi, M. I. (2014). *Creating an information systems security culture through an integrated model of employees compliance*. The University of Texas - Pan American.

Merhi, M. I., & Ahluwalia, P. (2014). The Role of Punishment and Task Dissonance in Information Security Policies Compliance. In *Americas Conference on Information Systems,Savannah* (pp. 1–10).

Merhi, M. I., & Midha, V. (2012). The impact of training and social norms on information security compliance: A pilot study. In *International Conference on Information Systems, ICIS 2012* (Vol. 5, pp. 4183–4193).

Ministry of Higher Education. (2018). MoHE - Institution. Retrieved January 13, 2018, from http://mohe.gov.my/en/institution

Nenad, R. (2013). Parliamentary control of security information agency in terms of security culture: State and problems. *Zbornik Radova Pravnog Fakulteta, Novi Sad*, *47*(3), 475–492. http://doi.org/10.5937/zrpfns47-4960

Ngo, L. (2008). IT Security Culture Transition Process. *Encyclopedia of Information Ethics and Security*, 319–325.

Ngo, L., Zhou, W., Chonka, A., & Singh, J. (2009). Assessing the level of I.T. security culture improvement: Results from three Australian SMEs. *IECON Proceedings (Industrial Electronics Conference)*, 3189–3195. http://doi.org/10.1109/IECON.2009.5415313

Ngo, L., Zhou, W., & Warren, M. (2005). Understanding Transition towards Information Security Culture Change. *Proceeding of the 3rd Australian Computer, Network & Information Forensics Conference, Edith Cowan University, School of Computer and Information Science*.

Niekerk, J. Van, & Solms, R. Von. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. *Issa*, 1–13.

Niekerk, J. Van, & Solms, R. Von. (2006). Understanding Information Security Culture: A Conceptual Framework. In *Proceedings of ISSA 2006* (pp. 1–10).

Niekerk, J. Van, & Solms, R. Von. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. http://doi.org/10.1016/j.cose.2009.10.005

Noorman Masrek, M., Nazrin Harun, Q., & Khairulnizan Zaini, M. (2017). Information Security Culture for Malaysian Public Organization: A Conceptual Framework. In *Proceedings of INTCESS 2017 4th International Conference on Education and Social Sciences* (pp. 156–166).

Nunnally, J., & Bernstein, I. (1994). *Psychometric Theory, 3rd edn, 1994. McGraw-Hill, New York* (Vol. 3).

OECD. (2002). *OECD Guidelines for the Security of Information Systems and Networks. OECD Digital Economy Papers No. 102*. Retrieved from http://www.oecd.org/internet/ieconomy/15582260.pdf

Okere, I., van Niekerk, J., & Carroll, M. (2012). Assessing Information Security Culture: A Critical Analysis of Current Approaches. *2012 Information Security for South Africa*. http://doi.org/10.1109/ISSA.2012.6320442

Olusegun, O. J., & Ithnin, N. B. (2013). " People Are the Answer to Security ": *Ijcsis*, *11*(8), 57–65.

Oost, D., & Chew, E. (2007). *Investigating the Concept of Information Security Culture*. *School of Management*. IGI Global. Retrieved from http://www.researchgate.net/publication/228830555_Investigating_the_Concept_of_Information_Security_Culture

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers and Security*, *31*(5), 673–680. http://doi.org/10.1016/j.cose.2012.04.004

Parsons, J. (1996). An Information Model Based on Classification Theory. *Management Science*, *42*(10), 1437–1453. http://doi.org/10.1287/mnsc.42.10.1437

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information Security Decision Making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117–129. http://doi.org/10.1177/1555343415575152

Parsons, K., Mccormac, A., Butavicius, M., & Ferguson, L. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment*. *Commonwealth of Australia*.

Paternoster, R., & Simpson, S. S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review*. http://doi.org/10.2307/3054128

Pavlou, P. A., & Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *Mis Quarterly*, *30*(1), 115–143. http://doi.org/10.2307/25148720

Petter, S., Straub, D., & Rai, A. (2007). Specifying Formative Constructs in Information Systems Research Author(s): *MIS Quarterly*, *31*(4), 623–656. http://doi.org/10.2307/25148814

Pevchikh, E. O. R. (2015). *Information Security Culture : Definition, Frameworks and Assessment A Systematic Literature Review*. Luleå University of Technology.

Pfeffer, J., & Sutton, R. I. (2000). *The knowing-doing gap : how smart companies turn knowledge into action*. Harvard Business School Press.

Pham, H.-C., El-Den, J., & Richardson, J. (2016). Stress-based security compliance model – an exploratory study. *Information & Computer Security Iss Computer Security*, *24*(2), 326–347. Retrieved from https://doi.org/10.1108/ICS-10-2014-0067

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. *The Journal of Applied Psychology*, *88*(5), 879–903. http://doi.org/10.1037/0021-9010.88.5.879

Podsakoff, P. M., Mackenzie, S. B., & Podsakoff, N. P. (2012). Sources of Method Bias in Social Science Research and Recommendations on How to Control It. *Annu. Rev. Psychol*, *63*, 539–69. http://doi.org/10.1146/annurev-psych-120710-100452

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: problems and prospects. *Journal of Management*. http://doi.org/10.1177/014920638601200408

Polites, G. L., Roberts, N., & Thatcher, J. (2012). Conceptualizing models using multidimensional constructs: a review and guidelines for their use. *European Journal of Information Systems*, *21*(1), 22–48. http://doi.org/10.1057/ejis.2011.10

Poll, H. (2015). *2015 Vormetric Insider Threat Report Trends and Future Directions in Data Security*.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers and Security*, *26*(3), 229–237. http://doi.org/10.1016/j.cose.2006.10.004

Pratt, T. C., Cullen, F. T., Sellers, C. S., Thomas Winfree, L., Madensen, T. D., Daigle, L. E., … Gau, J. M. (2010). *The Empirical Status of Social Learning Theory: A Meta-Analysis*. *JQ: Justice Quarterly* (Vol. 27). http://doi.org/10.1080/07418820903379610

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. http://doi.org/10.3758/BRM.40.3.879

Privacy Rights Clearinghouse. (2011). Privacy Rights Clearinghouse.

Privacy Rights Clearinghouse. (2014). Privacy Rights Clearinghouse. Retrieved January 17, 2017, from https://www.privacyrights.org/data-breaches

PWC. (2008). *Security Breaches Survey 2008. Enterprise and Regulatory Reform (BERR)*. Retrieved from http://www.eurim.org.uk/activities/ig/voi/DBERR.pdf

PWC. (2015). *2015 Information Security Breaches Survey*. Retrieved from https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

PWC. (2016). *The Global State of Information Security Survey 2016*.

Ramachandran, S., Rao, C., Goles, T., Dhillon, G., & Rao, V. S. (2013). Variations in Information Security Cultures across Professions: A Qualitative Study. *Communications of the Association for Information Systems*, *33*(11), 163–204.

Ramachandran, S., Rao, S. V., & Goles, T. (2008). Information security cultures of four professions: A comparative study. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. http://doi.org/10.1109/HICSS.2008.201

Ramachandran, S., & Rao, S. V. (2006). Security Cultures in Organizations : A Theoretical Model, 3460–3464.

Ratnamalala, N., & Marett, K. (2014). The impact of computer monitoring on policy compliance: An agency and stewardship view. *Americas Conference on Information Systems*, 1–9.

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*. http://doi.org/10.1109/ISSA.2014.6950492

Reid, R., Van Niekerk, J., & Renaud, K. (2014). Information security culture: A general living systems theory perspective. *2014 Information Security for South Africa*, 1–8. http://doi.org/10.1109/ISSA.2014.6950493

Renaud, K., & Goucher, W. (2014). The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8533 LNCS*, 361–372. http://doi.org/10.1007/978-3-319-07620-1_32

Report, T. T. (2019). Data Breach Hits Malaysian University, Personal Data Leaked. Retrieved January 28, 2019, from https://www.thethreatreport.com/data-breach-hits-malaysian-university-personal-data-leaked/

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7–8), 241–253. http://doi.org/10.1016/j.cose.2008.07.008

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826. http://doi.org/10.1016/j.cose.2009.05.008

Rhodes, K. A. (2001). Operations security awareness: the mind has no firewal. *Computer Security*, *18*(3), 27–36.

Richardson, R. (2011). 2010/2011 Computer Crime and Security Survey.

Ringle, C. M., Sarstedt, M., & Straub, D. (2012). A critical look at the use of PLS-SEM in MIS Quarterly. *MIS Quarterly (MISQ)*, *36*(1), iii–xiv. http://doi.org/10.3200/JOEB.79.4.213-216

Ringle, C. M., Wende, S., & Becker, J.-M. (2015). SmartPLS 3. Bönningstedt: SmartPLS. Retrieved from http://www.smartpls.com

Robbins, S. P., Odendaal, A., & Roodt, G. (2003). Organisational behaviour : global and Southern African perspectives. Cape Town : Pearson Education South Africa, 2003.

Robert, R. (2011). 201/2011 Computer Crime and Security Survey, 44. Retrieved from www.gocsi.com

Roberts, N. & Grover, V. (2009). Theory development in Information Systems research using Structural Equation Modeling: Evaluation and recommendations. In *Dwivedi, Y.K., Lal, B., Williams, M.D., Schneberger, S.L. & Wade, M.R. (Eds.), on Contemporary Theoretical Models in Information Systems, Hershey*. IGI Global.

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 and Security*, *43*, 90–110. http://doi.org/10.1016/j.cose.2014.03.004

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security*, *59*, 26–44. http://doi.org/10.1016/j.cose.2016.01.004

Rogers, R. W. (1983). Rogers, RW - Cognitive and physiological processes.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers and Security*, *26*(1), 56–62. http://doi.org/10.1016/j.cose.2006.10.008

Rungtusanatham, M., Miller, J. W., & Boyer, K. K. (2014). Theorizing, testing, and concluding for mediation in SCM research : Tutorial and procedural recommendations. *Journal of Operations Management*, *32*, 99–113.

Ryan, J. (2004). Information security tools and practices: what works? *IEEE Transactions on Computers*, *53*(4).

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. http://doi.org/10.1016/j.cose.2015.05.012

Sarstedt, M., Ringle, C. M., Smith, D., Reams, R., & Hair, J. F. J. (2014). Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers. *Journal of Family Business Strategy*, *5*(1), 105–115. http://doi.org/10.1016/J.JFBS.2014.01.002

Sasse, M. A., Brostoff, S., & Weirich, D. (2004). Transforming the "Weakest Link": A Human-Computer Interaction Approach for Usable and Effective Security. *BT Technology Journal*, *19*(31), 122.

Schein, E. H. (1985). Organizational culture and leadership: A dynamic view. *Organization Studies*, *7*, 199–201. http://doi.org/10.1177/017084068600700208

Schein, E. H. (1992). *Organizational culture and leadership*. *SF JosseyBass Senge P* (Vol. 7).

Schein, E. H. (1999). *The Corporate Culture Survival Guide*. Jossey-Bass Inc.

Schein, E. H. (2004). Organizational Culture and Leadership. *Leadership*, *7*, 437. http://doi.org/10.1080/09595230802089917

Schlienger, T., & Teufel, S. (2002). Information Security Culture - The Socio-Cultural Dimension in Information Security Management. *Security in the Information Society: Visions and Perspectives. IFIP TC11 International Conference on Information Security (Sec2002)*, 191–201.

Schlienger, T., & Teufel, S. (2003a). Analyzing information security culture: Increased trust by an appropriate information security culture. *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA, 2003–Janua*, 405–409. http://doi.org/10.1109/DEXA.2003.1232055

Schlienger, T., & Teufel, S. (2003b). Information security culture: from analysis to change. *South African Computer Journal*, *31*, 46–52.

Schlienger, T., & Teufel, S. (2005). Tool supported management of information security culture. In *IFIP Advances in Information and Communication Technology* (pp. 65–77).

Schultz, E. (2005). The human factor in security. *Computers & Security*, *24*(6), 425–426.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers and Security*, *21*(6), 526–531. http://doi.org/10.1016/S0167-4048(02)01009-X

Shahibi, M. S., Rohana Mohamad Rashid, Shamsul Kamal Wan Fakeh, Wan Ab Kadir Wan Dollah, & Juwahir Ali. (2012). Determining Factors Influencing Information Security Culture Among ICT Librarians. *Journal of Theoretical and Applied Information Technology*, *37*(1), 132–140.

Shahri, A. B., Ismail, Z., & Rahim, N. Z. A. (2013). Security culture and security awareness as the basic factors for security effectiveness in health information systems. *Jurnal Teknologi (Sciences and Engineering)*, *64*(2), 7–12. http://doi.org/10.11113/jt.v64.2212

Sharif, H., Ismail, Z., & Masrom, M. (2007). Users ' Perception on the Information Security Policy of the Institutions of Higher Learning.

Shaw, R. M. (2012). The Influence of Organizational Culture on Employee Attitudes Towards Information Security Policy, (March), 124.

Shawn Logan. (2017). University of Calgary pays hackers $20,000 after ransomware attack | Calgary Herald. Retrieved January 17, 2017, from http://calgaryherald.com/news/local-news/university-of-calgary-pays-hackers-20000-after-ransomware-attack

Sherif, E., & Furnell, S. (2015). A Conceptual Model for Cultivating an Information Security Culture. *International Journal for Information Security Research*, *5*(2), 565–573.

Sherif, E., Furnell, S., & Clarke, N. L. (2015). An Identification of Variables Influencing the Establishment of Information Security Culture. In *3rd International Conference on Human Aspects of Information Security, Privacy and Trust, HAS 2015* (Vol. 9190, pp. 436–448). http://doi.org/10.1007/978-3-319-20376-8

Silvius, A., & Dols, T. (2012). Factors influencing Non-Compliance behavior towards Information Security Policies. *CONF-IRM 2012 Proceedings*.

Sin, L. Y. M., Cheung, W. H., & Lee, R. (1999). Methodology in cross cultural consumer research: A review and critical assessment. *Journal of International Consumer Marketing*, *11*(4), 75–96.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. http://doi.org/10.1016/j.im.2013.08.006

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. In *IFIP International Federation for Information Processing* (Vol. 232, pp. 133–144). http://doi.org/10.1007/978-0-387-72367-9_12

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64–71. http://doi.org/10.1109/MC.2010.35

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. http://doi.org/10.1108/09685220010371394

Siponen, M. T. (2005). Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods. *Information and Organization*, *15*(4), 339–375. http://doi.org/10.1016/j.infoandorg.2004.11.001

Siponen, M., & Vance, A. (2010). Neutralizaiton: New Insights into the Problem of Employee Information Systems Security. *MIS Quarterly*, *34*(3), 487–502. http://doi.org/Article

Smith, E. E., & Medin, D. L. (1981). Categories and concepts. *Cognitive Science Series*. http://doi.org/10.2307/414206

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13. http://doi.org/10.1016/j.cose.2015.10.006

Sommestad, T., & Hallberg, J. (2013). A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance, 257–271.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance. *Information Management & Computer Security*, *22*(1), 42–75. http://doi.org/10.1108/IMCS-08-2012-0045

Sommestad, T., Karlzén, H., & Hallberg, J. (2014). The sufficiency of the theory of planned behavior for explaining information security policy compliance.

Sommestad, T., Karlzén, H., & Hallberg, J. (2017). The Theory of Planned Behavior and Information Security Policy Compliance. *Journal of Computer Information Systems*, 1–10.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, *48*(7), 296–302. http://doi.org/10.1016/j.im.2011.07.002

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly (MISQ)*, *34*(3), 503–522.

Standard, I. (2005). *International Standard ISO / IEC* (Vol. 2005).

Stanton, J. M., Mastrangelo, P. R., Stam, K. R., & Jolton, J. (2004). Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices. *Behavioral Information Security*, (August), 1388–1394.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124–133. http://doi.org/10.1016/j.cose.2004.07.001

Stephen P. Robbins. (2001). *Organizational Behavior* (9th ed.). Prentice Hall International, Inc.

Steve Durbin. Insiders are today's biggest security threat - Recode, Security Voices (2016). Retrieved from http://www.recode.net/2016/5/24/11756584/cyber-attack-data-breach-insider-threat-steve-durbin

Straub, D. W. (1989). Validating Instruments in MIS Research. *MIS Quarterly*, *13*(2), 147–169.

Straub, D. W., & Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(4), 417. http://doi.org/Doi 10.2307/249551

Tabachnick, B. G., & Fidell., L. S. (2001). *Using multivariate statistics* (4th ed.). Boston: Allyn and Bacon.

Talib, Y. Y. A., & Dhillon, G. (2015). Employee ISP Compliance Intentions : An Empirical Test of Empowerment. *Proceedings of the 36th International Conference on Information Systems (ICIS)*.

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Inf Technol Manag*, *17*, 179–186.

Tehseen, S., & Gadar, K. (2017). Assessing Cultural Orientation as a Reflective-Formative Second Order Construct -A Recent PLS-SEM Approach. *Review of Integrative Business and Economics ResearchOnlineCDROM*, *6*(2), 38–63.

Tehseen, S., Ramayah, T., & Sajilan, S. (2017). Testing and Controlling for Common Method Variance: A Review of Available Methods. *Journal of Management Sciences*, *4*(2), 142–168. http://doi.org/10.20547/jms.2014.1704202

Tejay, G., & Dhillon, G. (2005). Developing Measures of Information Security. In *The Fourth Annual Workshop on E-Business, Las Vegas, NV*.

Temesgen, G., Lessa, & Ferede, L. (2011). Information Security Culture in Public Hospitals : The Case of Hawassa Referral Hospital. *The African Journal of Information Systems*, *3*(3).

Teufel, S., & Teufel, B. (2015). Crowd Energy Information Security Culture - Security Guidelines for Smart Environments. In *Proceedings - 2015 IEEE International Conference on Smart City, SmartCity 2015, Held Jointly with 8th IEEE International Conference on Social Computing and Networking, SocialCom 2015, 5th IEEE International Conference on Sustainable Computing and Communic* (pp. 123–128). http://doi.org/10.1109/SmartCity.2015.58

The Hacker News. (2017a). Protect Against WannaCry: Microsoft Issues Patch for Unsupported Windows (XP, Vista, 8,...). Retrieved May 14, 2017, from http://thehackernews.com/2017/05/wannacry-ransomware-windows.html

The Hacker News. (2017b). WannaCry Kill-Switch(ed)? It's Not Over! WannaCry 2.0 Ransomware Arrives. Retrieved May 15, 2017, from http://thehackernews.com/2017/05/wannacry-ransomware-cyber-attack.html

The Sun Daily. (2017). WannaCry ransomware attack in Malaysia confirmed. Retrieved May 17, 2017, from http://www.thesundaily.my/news/2017/05/16/wannacry-ransomware-attack-malaysia-confirmed

The Telegraph. (2017). Government under pressure after NHS crippled in global cyber attack as weekend of chaos looms. Retrieved May 14, 2017, from http://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/

Thomson, K.-L. (2010). Information Security Conscience: a precondition to an Information Security Culture? *Journal of Information System Security*, *6*(4), 5–19.

Thomson, K.-L., Von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11. http://doi.org/10.1016/S1361-3723(06)70430-4

Times, N. S. (2019a). Data leak: Breach too far. Retrieved June 2, 2019, from https://www.nst.com.my/opinion/leaders/2019/01/454849/data-leak-breach-too-far

Times, N. S. (2019b). UiTM to probe claims of data breach. Retrieved January 25, 2019, from https://www.nst.com.my/news/nation/2019/01/454429/uitm-probe-claims-data-breach

Tolah, A., Furnell, S. M., & Papadaki, M. (2017). A Comprehensive Framework for Cultivating and Assessing Information Security Culture, (Haisa), 52–64.

Tsohou, A., & Holtkamp, P. (2018). Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology and People*, *31*(2), 1047–1068. http://doi.org/10.1108/ITP-02-2017-0052

UCF Data Breach | IdentityForce. (2017). University of Central Florida (UCF) Data Breach Affects 63,000 Students and Staff. Retrieved January 17, 2017, from https://www.identityforce.com/blog/ucf-data-breach-affects-63000

Uffen, J., Guhr, N., & Breitner, M. H. (2012). Personality traits and information security management: An empirical study of information security executives. In *International Conference on Information Systems, ICIS 2012* (Vol. 2, pp. 1188–1209).

UKM. (2016). Dasar Keselamatan Teknologi Maklumat dan Komunikasi Universiti Kebangsaan Malaysia.

UMP. (2015). *Dasar Keselamatan ICT 2015 UMP*.

Van Niekerk, J., & Von Solms, R. (2013). A theory based approach to information security culture change. *Information (Japan)*, *16*(6B), 3907–3930.

Vance, A. (2012). IS Security Policy Violations: A Rational Choice Perspective. *Journal of Organizational and End User Computing*, *24*(1), 21–41. http://doi.org/10.4018/joeuc.2012010102

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. http://doi.org/10.1016/j.im.2012.04.002

Veiga, A., Martins, N., & Eloff, J. H. P. (2007). Information security culture – validation of an assessment instrument, *11*(1).

Veiga, A. Da. (2008). *Cultivating and Assessing Information Security Culture*. University of Pretoria.

Veiga, A. Da. (2015a). An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security- Positive Culture An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security- Positive Culture. In *Human Aspects of Information Security & Assurance (HAISA 2015)* (pp. 95–107).

Veiga, A. Da. (2015b). The Influence of Information Security Policies on Information Security Culture : Illustrated through a Case Study, (Haisa), 22–33.

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425–478. http://doi.org/10.2307/30036540

Verizon Business. (2011). 2011 Data Breach Investigations Report (DBIR). *Trends*, 1–72. http://doi.org/10.1109/CyberSec.2012.6246130

Von Solms, B. (2000). Information Security — The Third Wave? *Computers & Security*, *19*(7), 615–620. http://doi.org/10.1016/S0167-4048(00)07021-8

Von Solms, B. (2006). Information Security - The Fourth Wave. *Computers and Security*, *25*(3), 165–168. http://doi.org/10.1016/j.cose.2006.03.004

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security*, *23*(4), 275–279. http://doi.org/10.1016/j.cose.2004.01.013

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, *23*(3), 191–198. http://doi.org/10.1016/j.cose.2004.01.012

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101–105. http://doi.org/10.1057/ejis.2009.12

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44*(March 2016), 1–15. http://doi.org/10.1016/j.cose.2014.04.005

Webb, T. L., & Sheeran, P. (2006). Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. *Psychological Bulletin*, *132*(2), 249–268. http://doi.org/10.1037/0033-2909.132.2.249

Wenzel, M. (2004). The social side of sanctions: Personal and social norms as moderators of deterrence. *Law and Human Behavior*, *28*(5), 547–567. http://doi.org/10.1023/B:LAHU.0000046433.57588.71

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*(1), 4–19. http://doi.org/10.1108/09685220910944722

Werner, L., & Campbell, D. T. (1970). Translating,working through interpreters and the problem of decentering. In *American handbook of methods in cultural anthropology, ed. R. Naroll and R. Cohen* (pp. 398–420). New York: Natural History Press.

Westland, C. J. (2010). Lower bounds on sample size in structural equation modeling. *Electronic Commerce Research and Applications*, *9*(6), 476–487.

Wetzels, M., Odekerken-Schröder, G., & Oppen, C. van. (2009). Using Pls Path Modeling for Assessing Hierarchical C Onstruct M Odels : G Uidelines and E Mpirical, *33*(1), 177–195. http://doi.org/Article

Whitman, M. E. (2008). Security Policy: From Design to Maintenance. *Advances in Management Information Systems*, *11*, 123–151.

Williams, P. A. H. (2008). In a "trusting" environment, everyone is responsible for information security. *Information Security Technical Report*, *13*(4), 207–215.

Williams, P. A. H. (2009a). Capturing Culture in Medical Information Security Research. *Methodological Innovations Online*, *4*(3), 15–26. http://doi.org/10.4256/mio.2010.0003

Williams, P. A. H. (2009b). What does security culture look like for small organizations? In *Australian Information Security Management Conference* (pp. 48–54).

Willison, R., & Siponen, M. T. (2009). Overcoming the Insider: Reducing Employee Computer Crime Through Situational Crime Prevention. *Communications of the ACM*, *52*(9), 133–137. http://doi.org/10.1145/1562164.1562198

Wilson, B., & Henseler, J. (2007). Modeling reflective higher-order constructs using three approaches with PLS path modeling: a Monte Carlo comparison. In *Australian and New Zealand Marketing Academy Conference* (pp. 791–800).

Wiser.my. (2017). Virus Ransomware WannaCry Sudah Muncul Di Malaysia- Pakar Sekuriti | Laporan Teknologi & Gajet. Retrieved May 15, 2017, from https://wiser.my/virus-ransomware-wannacry-sudah-muncul-di-malaysia/

Wold, H. (1982). Soft modelling: the basic design and some extensions. *Systems under Indirect Observation: Causality-Structure-Prediction*, 1–54.

Wold, H., & Noonan, R. (1983). Evaluating School Systems Using Partial Least Squares. *Evaluation in Education*, *7*, 219–364.

Wong, C. S., Law, K. S., & Huang Guo-Hua, G. H. (2008). On the importance of conducting construct-level analysis for multidimensional constructs in theory development and testing. *Journal of Management*, *34*(4), 744–764. http://doi.org/10.1177/0149206307312506

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security*, *16*(November), 315–331. http://doi.org/10.1080/10658980701788165

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. http://doi.org/10.1016/j.chb.2008.04.005

Wright, R. T., Campbell, D. E., Thatcher, J. B., & Roberts, N. (2012). Operationalizing Multidimensional Constructs in Structural Equation Modeling: Recommendations for IS Research. *Comunications of the Association for Information System*, *30*(June 2012 (article 23)), 367–412.

Xue, Y., Liang, H., & Wu, L. (2011). Punishment, Justice, and Compliance in Mandatory IT Settings. *Information Systems Research*, *22*(2), 400–414. http://doi.org/10.1287/isre.1090.0266

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. http://doi.org/10.1016/j.dss.2016.09.009

Yu, D. F., Lee, D. T., & Woo, J. (2004). Issues and challenges of instrument translation. *Western Journal of Nursing Research*, *26*, 307–320.

Zakaria, O. (2004). Understanding challenges of information security culture: a methodological issue. In *2nd Australian Information Security Management Conference* (pp. 83–93).

Zakaria, O. (2006). Internalisation of information security culture amongst employees through basic security knowledge. *IFIP International Federation for Information Processing*, *201*, 437–441. http://doi.org/10.1007/0-387-33406-8_38

Zakaria, O. (2007). *Investigating information security culture challenges in a public sector organisation : Malaysian a case*. University of London.

Zakaria, O. (2013). *Information Security Culture: A Human Firewall Approach*. LAP Lambert Academic Publishing.

Zakaria, O., & Gani, A. (2003). A Conceptual Checklist of Information Security Culture. In *Proceeding of the 2nd European Conference on Information Warfare and Security, Reading, United Kingdom* (pp. 365–371).

Zakaria, O., Jarupunphol, P., & Gani, A. (2003). Paradigm Mapping for Information Security Culture Approach. *Proceedings 4th Australian Information Warfare & IT Security Conference*, (November), 137–149.

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and Truths about Mediation Analysis. *Journal of Consumer Research*, *37*(2), 197–206. http://doi.org/10.1086/651257

Zikmund, W. G. (2003). *Business Research Methods*. Mason, Ohio: Thomson/South-Western.

Zurko, M. E., Kaufman, C., Spanbauer, K., & Bassett, C. (2002). Did you ever have to make up your mind? What Notes users do when faced with a security decision. In *18th Annual Computer Security Applications Conference, 2002. Proceedings.* (pp. 371–381). IEEE Comput. Soc. http://doi.org/10.1109/CSAC.2002.1176309

APPENDIX A
EXAMPLE OF E-MAIL FOR DATA COLLECTION

Information Security Culture Survey

AKHYARI BIN NASIR

Thu 11/30/2017 7:38 AM

To:fatimahsfz@iium.edu.my <fatimahsfz@iium.edu.my>;

1 attachments (623 KB)

Official Letter.pdf;

Dear Dr. Siti Fatimah Binti Zakaria,

My name is Akhyari Nasir, a postgraduate student from Universiti Malaysia Pahang (UMP) under supervision of Assoc. Prof. Dr. Ruzaini Abdullah Arshah and Assoc. Prof. Dr. Mohd. Rashid Ab Hamid. My Student ID is PCC 16001. Attached with this email is a letter of declaration and permission from Faculty of Computer Systems and Software Engineering, UMP for your reference.

I am writing to you to request your help to be a respondent in my brief survey. It only takes approximately 10 minutes to finish. My study is regarding Information Security Culture and Employee's Information Security Compliance Behavior towards ICT Security Policy in Malaysian Universities. Therefore, your responses and information are very important in this study. All information you provide will be treated as strictly confidential. Your responses will be presented in aggregate and no individual responses will be reported.

Please click on this link to participate ----> https://goo.gl/forms/uM89wPRmz20kRuC23

Information Security Culture and Employee's ICT Security Policy Compliance in Malaysian Public Universities

goo.gl

For Bahasa Malaysia version, please click ---> https://goo.gl/forms/QW0K1u7dMVpcgOqO2

Budaya Keselamatan Maklumat dan Kepatuhan Pekerja Terhadap Dasar Keselamatan ICT di Universiti Awam Malaysia

goo.gl

https://outlook.office.com/owa/?viewmodel=ReadMessageItem&ItemID=AAMkAGFkMGUyODAxLTZhYTYtNDE5OC1iNTI0LWI0Mzc0YTYwOGE2MwBGAAAAAADy1

Look forward to receiving your positive reply by taking this survey. Thank you very much.

Yours Truly,

AKHYARI NASIR
019-9804567
https://www.researchgate.net/profile/Akhyari_Nasir

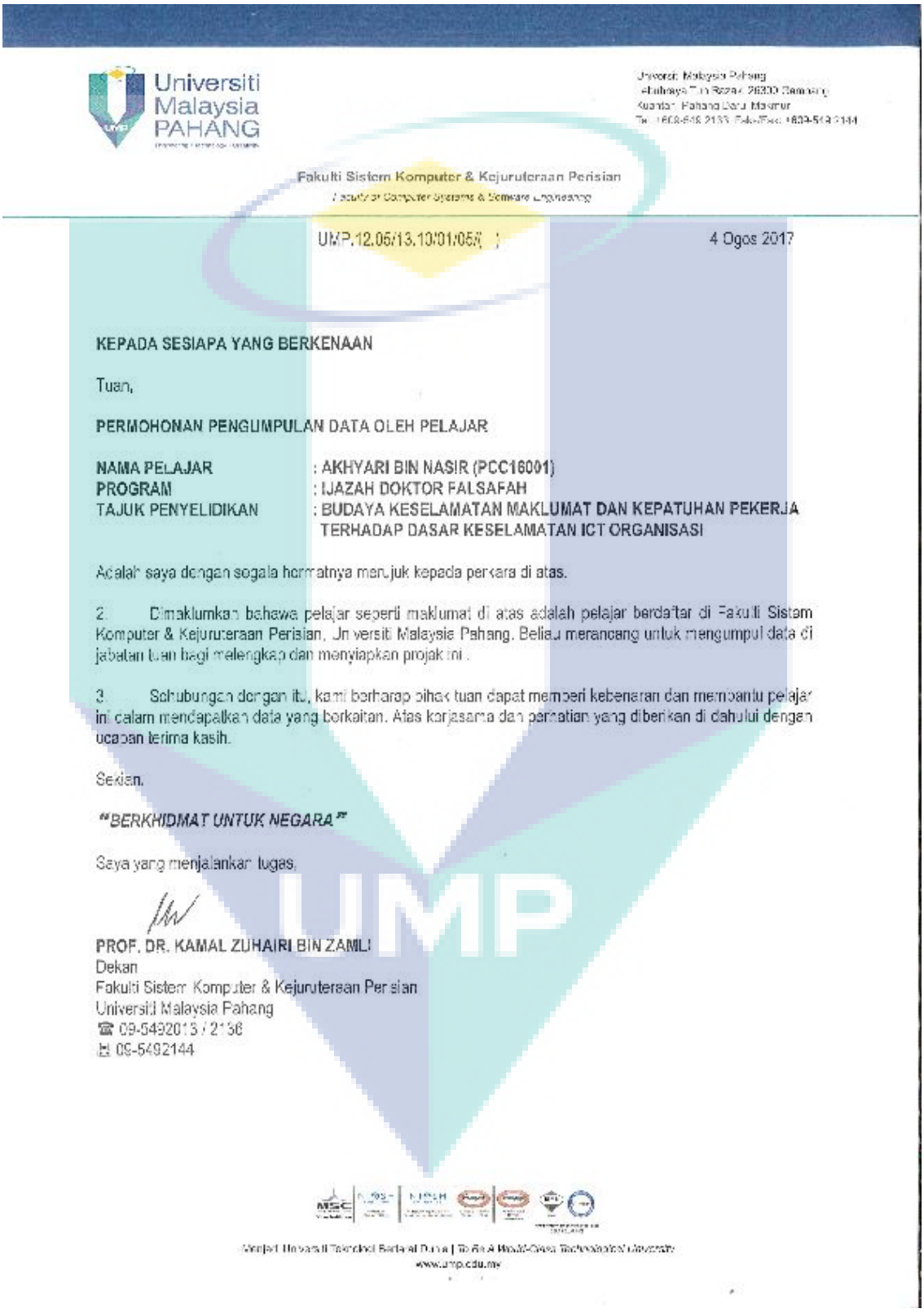
Akhyari bin Nasir (TATI University College, Cukai) on ...

www.researchgate.net

Akhyari bin Nasir of TATI University College, Cukai with expertise in Computer and Society is on ResearchGate. Read 8 publications, 2 answers, and contact Akhyari bin ...

https://outlook.office.com/owa/?viewmodel=ReadMessageItem&ItemID=AAMkAGFkMGUyODAxLTZhYTYtNDE5OC1iNTlCLWI0Mzc0YTYwOGE2MwBGAAAAAADy1

APPENDIX B
OFFICIAL LETTER FOR DATA COLLECTION



Universiti Malaysia PAHANG

Universiti Malaysia Pahang
Kuantan Pahang Darul Makmur

Fakulti Sistem Komputer & Kejuruteraan Perisian
Faculty of Computer Systems & Software Engineering

UMP.12.05/13.10/01/05( ) 4 Ogos 2017

KEPADA SESIAPA YANG BERKENAAN

Tuan,

PERMOHONAN PENGUMPULAN DATA OLEH PELAJAR

NAMA PELAJAR	: **AKHYARI BIN NASIR (PCC16001)**
PROGRAM	: **IJAZAH DOKTOR FALSAFAH**
TAJUK PENYELIDIKAN	: **BUDAYA KESELAMATAN MAKLUMAT DAN KEPATUHAN PEKERJA TERHADAP DASAR KESELAMATAN ICT ORGANISASI**

Adalah saya dengan segala hormatnya merujuk kepada perkara di atas.

2. Dimaklumkan bahawa pelajar seperti maklumat di atas adalah pelajar berdaftar di Fakulti Sistem Komputer & Kejuruteraan Perisian, Universiti Malaysia Pahang. Beliau merancang untuk mengumpul data di jabatan tuan bagi melengkap dan menyiapkan projek ini.

3. Sehubungan dengan itu, kami berharap pihak tuan dapat memberi kebenaran dan membantu pelajar ini dalam mendapatkan data yang berkaitan. Atas kerjasama dan perhatian yang diberikan di dahului dengan ucapan terima kasih.

Sekian.

"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan tugas,

PROF. DR. KAMAL ZUHAIRI BIN ZAMLI
Dekan
Fakulti Sistem Komputer & Kejuruteraan Perisian
Universiti Malaysia Pahang
☎ 09-5492013 / 2136
🖷 09-5492144

Peneraju Universiti Teknologi Berkesan Dunia | To Be A World-Class Technological University
www.ump.edu.my

APPENDIX C
SUMMARY OF FACTOR ANALYSIS FOR COMMON METHOD BIAS TEST

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	19.393	44.074	44.074	19.393	44.074	44.074
2	4.349	9.883	53.957	4.349	9.883	53.957
3	2.615	5.943	59.900	2.615	5.943	59.900
4	1.815	4.126	64.026	1.815	4.126	64.026
5	1.685	3.829	67.855	1.685	3.829	67.855
6	1.498	3.404	71.259	1.498	3.404	71.259
7	1.433	3.258	74.517	1.433	3.258	74.517
8	1.293	2.938	77.454	1.293	2.938	77.454
9	1.049	2.384	79.839	1.049	2.384	79.839
10	.803	1.825	81.664			
11	.736	1.672	83.336			
12	.615	1.397	84.732			
13	.567	1.288	86.021			
14	.499	1.135	87.156			
15	.466	1.059	88.215			
16	.404	.919	89.134			
17	.348	.791	89.925			
18	.332	.754	90.679			
19	.313	.712	91.391			
20	.303	.688	92.079			
21	.280	.636	92.715			
22	.257	.585	93.300			
23	.250	.567	93.868			
24	.235	.535	94.403			
25	.220	.499	94.902			
26	.210	.477	95.379			
27	.203	.460	95.840			
28	.177	.402	96.241			
29	.172	.390	96.632			
30	.162	.368	97.000			
31	.144	.327	97.327			
32	.141	.321	97.648			
33	.135	.306	97.954			
34	.121	.275	98.230			
35	.117	.265	98.495			
36	.110	.249	98.744			
37	.100	.227	98.971			
38	.089	.202	99.173			
39	.079	.180	99.353			
40	.071	.162	99.516			
41	.060	.137	99.653			
42	.055	.125	99.778			
43	.050	.113	99.891			
44	.048	.109	100.000			

Extraction Method: Principal Component Analysis.

APPENDIX D
DESCRIPTIVE STATISTICS FOR 7-POINT LIKERT SCALE ITEMS

Items	N	Mean	Std. Deviation	Skewness	Kurtosis
PCM1	604	5.43	1.472	-.829	.122
PCM2	604	5.69	1.266	-1.024	.831
PCM3	604	5.36	1.427	-.818	.204
PCM4	604	5.53	1.330	-.938	.605
RM1	604	5.77	1.089	-.936	1.079
RM2	604	5.62	1.073	-.651	.022
RM3	604	6.13	.919	-.960	.439
RM4	604	5.77	1.098	-.895	.790
SETA1	604	4.80	1.539	-.450	-.379
SETA2	604	4.83	1.516	-.442	-.414
SETA3	604	5.01	1.492	-.520	-.340
SETA4	604	5.15	1.411	-.652	-.002
TMC1	604	5.30	1.326	-.603	-.203
TMC2	604	5.42	1.274	-.567	-.333
TMC3	604	5.42	1.260	-.650	-.107
TMC4	604	5.67	1.195	-.827	.225
MON1	604	5.01	1.455	-.565	-.187
MON2	604	5.40	1.220	-.614	-.076
MON3	604	5.01	1.343	-.485	-.089
MON4	604	5.03	1.342	-.536	-.029
ISK1	604	5.44	1.215	-.564	-.233
ISK2	604	5.54	1.088	-.534	-.116
ISK3	604	5.61	1.102	-.655	-.119
ISK4	604	5.25	1.313	-.653	.047
ISK5	604	5.19	1.326	-.578	-.158
ISKS1	604	4.75	1.453	-.395	-.384
ISKS2	604	4.82	1.384	-.470	-.370
ISKS3	604	5.41	1.223	-.625	-.025
ISKS4	604	5.64	1.068	-.632	.138
ISKS5	604	5.85	1.014	-.735	.203
INT1	604	6.14	.910	-.841	-.098
INT2	604	6.09	.918	-.770	-.158
INT3	604	6.18	.884	-.856	-.012
INT4	604	6.18	.884	-.849	-.104

APPENDIX E
DESCRIPTIVE STATISTICS FOR 5-POINT LIKERT SCALE ITEMS

Items	N	Mean	Std. Deviation	Skewness	Kurtosis
ATT1	604	4.66	.534	-1.317	1.152
ATT2	604	4.61	.586	-1.534	3.127
ATT3	604	4.63	.542	-1.084	.152
ATT4	604	4.62	.549	-1.108	.223
NB1	604	4.26	.796	-.912	.646
NB2	604	4.24	.810	-.912	.699
NB3	604	4.13	.873	-.801	.283
SE1	604	3.66	.949	-.547	.065
SE2	604	3.71	.920	-.620	.307
SE3	604	3.69	.942	-.608	.231

APPENDIX F
UNIVARIATE AND MULTIVARIATE NORMALITY TEST RESULTS

Output of skewness and kurtosis calculation

```
Sample size:  604
Number of variables:  11

Univariate skewness and kurtosis
       Skewness     SE_skew    Kurtosis   SE_kurt
ATT  -1.0719426 0.09942199  0.13876524 0.1985194
INT  -0.7793339 0.09942199 -0.16080125 0.1985194
ISK  -0.4672404 0.09942199 -0.27632585 0.1985194
ISKS -0.4272698 0.09942199 -0.15480529 0.1985194
MON  -0.4584737 0.09942199 -0.22238308 0.1985194
NB   -0.8581137 0.09942199  0.64191648 0.1985194
PCM  -0.7842621 0.09942199  0.27634871 0.1985194
RM   -0.6523142 0.09942199  0.05100016 0.1985194
SE   -0.5784447 0.09942199  0.27708355 0.1985194
SETA -0.4755956 0.09942199 -0.19490822 0.1985194
TMC  -0.6170051 0.09942199 -0.16286057 0.1985194

Mardia's multivariate skewness and kurtosis
                  b          z p-value
Skewness  18.80482 1893.01809       0
Kurtosis 193.52827   36.71469       0
```

APPENDIX G
QUESTIONNAIRE

Information Security Culture and Employee's ICT Security Policy Compliance in Malaysian Public Universities

Dear Respondent,

This survey is conducted to collect data from public university's employees in Malaysia to study the influence of Information Security Culture (ISC) towards employee's Information and Communication Technology (ICT) Security Policy compliance behavior. It only takes approximately 10 minutes to finish. Please be open, honest and candid with your responses. Your responses are highly valuable for this study in improving the quality of culture and performance of information security in Malaysian Public Universities. All information you provide will be treated as strictly confidential. Your responses will be presented in aggregate and no individual responses will be reported.

Conducted by:
Akhyari Nasir (Post-graduate student)
Faculty of Computer Systems & Software Engineering (FSKKP), Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300 Kuantan, Pahang, Malaysia
Email: akhyari@tatiuc.edu.my; Phone No.: +6 019804567

Supervisors:
1. Associate Professor Dr. Ruzaini Abdullah Arshah
Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300 Kuantan, Pahang, Malaysia
Email: ruzaini@ump.edu.my; Phone No.: +6019841428
2. Associate Professor Dr. Mohd Rashid Ab Hamid
Faculty of Industrial Management, Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300 Kuantan, Pahang, Malaysia
Email: rashid@ump.edu.my; Phone No.: +60143371786

*Required

Section A: Demographic Information

This section is to collect demographic information about you and your firm. Please choose the appropriate answers and where relevant, specify your answer.

1.

1. Gender *

Mark only one oval.

- ◯ Male
- ◯ Female

2. **2. Age** *

Mark only one oval.

- ◯ 18 – 24 Years
- ◯ 25 – 34 Years
- ◯ 35 – 44 Years
- ◯ 45 – 54 Years
- ◯ 55 Years and over
- ◯ Other: _____

3. **3. Race** *

Mark only one oval.

- ◯ Malay
- ◯ Chinese
- ◯ Indian
- ◯ Other: _____

4. **4. Highest education you have achieved** *

Mark only one oval.

- ◯ High School
- ◯ College
- ◯ Diploma
- ◯ Degree
- ◯ Master Degree
- ◯ PhD
- ◯ Other: _____

5. **5. Name of University you are currently work for** *

Mark only one oval.

- Universiti Malaya (UM)
- Universiti Teknologi MARA (UiTM)
- Universiti Sains Malaysia (USM)
- Universiti Kebangsaan Malaysia (UKM)
- Universiti Putra Malaysia (UPM)
- Universiti Teknologi Malaysia (UTM)
- Universiti Islam Antarabangsa Malaysia (UIAM)
- Universiti Utara Malaysia (UUM)
- Universiti Malaysia Sarawak (UNIMAS)
- Universiti Malaysia Sabah (UMS)
- Universiti Pendidikan Sultan Idris (UPSI)
- Universiti Sains Islam Malaysia (USIM)
- Universiti Teknikal Malaysia Melaka (UTeM)
- Universiti Malaysia Perlis (UniMAP)
- Universiti Malaysia Pahang (UMP)
- Universiti Sultan Zainal Abidin (UniSZA)
- Universiti Pertahanan Nasional Malaysia (UPNM)
- Universiti Malaysia Kelantan (UMK)
- Universiti Malaysia Terengganu (UMT)
- Universiti Tun Hussein Onn Malaysia (UTHM)
- Universiti Sultan Azlan Shah (USAS)
- Other: _____

6. **6. Experience in this University** *

Mark only one oval.

- Less than 2 Years
- 2 to 5 Years
- 5 to 10 Years
- 10 to 20 Years
- 20 Years and over

7. **7. Service Type** *

Tick all that apply.

- [ ] Academic
- [ ] Management
- [ ] Administration/Support
- [ ] Other: _____

8. **8. What profession do you consider yourself to be a part of?**
Mark only one oval.

- ◯ IT Professional (e.g: ICT Manager, Programmer, System Administrator, Web/Multimedia Administrator or any related IT jobs)
- ◯ Non-IT Professional

Section B1: Aspects of Information Security Culture in Organization

In this section, the researcher is interested to assess particular aspects of information security culture in the organization. Please indicate the number that best matches the degree to which you agree or disagree with the statements (where 1- Strongly disagree, and 7- Strongly agree).

ICT Security Policy

9. **1. My organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

10. **2. My organization has established rules of behavior for use of ICT resources.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

11. **3. My organization has specific guidelines that govern what employees are allowed to do with their computers.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

12. **4. My organization has specific guidelines that describe acceptable use of e-mail.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

Information Security Risk Management

13. **5. I believe that threats to ICT assets are controlled adequately in my organizations.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agre

14. **6. I believe the risk management processes are adequate to identify the risks that could negatively impact on the confidentiality, integrity and availability of our ICT assets.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

15. **7. It is important to understand the threats and vulnerabilities to information assets in my work environment.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

16. **8. I believe that my organization has appropriate plans for risk management.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

Security Education, Training and Awareness (SETA)

17. **9. In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

18. **10. In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

19. **11. My organization provides training to help employees improve their awareness of computer and information security issues.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

20. **12. My organization educates employees on their computer security responsibilities.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

Top Management Commitment

21. **13. I believed senior managers of my organization have articulated a clear vision about information security.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

22. **14. I believed senior managers of my organization have formulated a clear strategy for achieving a high degree of information security.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

23. **15. I believed senior managers of my organization have established clear goals and objectives for achieving a high degree of information security.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

24. **16. Top management considers information security an important organizational priority.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

This section continues to the next page...

Section B2: Aspects of Information Security Culture in Organization

In this section, the researcher is interested to assess particular aspects of information security culture in the organization. Please indicate the number that best matches the degree to which you agree or disagree with the statements (where 1- Strongly disagree, and 7- Strongly agree).

Monitoring

25. **17. I believe that my organization conducts periodic audits to detect the use of unauthorized software on its computers.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

26. **18. I believe that employee computing activities are monitored by my organization.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

27. **19. I believe that my organization reviews logs of employees' computing activities on a regular basis.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

28. **20. I believe that my organization monitors any modification or altering of computerized data by employees.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

Information Security Knowledge

29. **21. There are adequate information security specialist/coordinator/person-in-charge throughout my organization to ensure the implementation of information security controls.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

30. **22. I believe that information security controls implemented in my organization are in line with appropriate practice guidelines to secure information assets.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

31. **23. I believe that my organization has adequate knowledge of information security to implement information security programs and campaigns.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

32. **24. Information security programs organized by the organization have helped me improving my information security knowledge.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

33. **25. Information security programs organized by the organization have helped me improving my information security skills.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

Information Security Knowledge Sharing

34. **26. I frequently share my information security knowledge in my working place in order to decrease information security risk.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

35. **27. I participate in information security knowledge sharing in order to keep myself up to date.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

36. **28. I think information security knowledge sharing helps me to understand the usefulness of ICT security policies in my organization.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

37. **29. I think information security knowledge sharing is an effective approach to mitigate the risk of information security breaches.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

38. **30. I think information security knowledge sharing is a valuable practice in organizations.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

SECTION C: INFORMATION SECURITY BEHAVIOR

In this section of the survey, the researcher is interested in assessing particular aspects of information security behavior. Please provide your answer according to the given scale.

Attitude

Please indicate the number that best matches the degree to which you agree or disagree with the statements (where 1-Strongly disagree, and 5-Strongly agree).

39. **1. Following the organization's ICT Security Policy is important.** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

40. **2. Following the organization's ICT Security Policy is necessity.** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

41. **3. Following the organization's ICT Security Policy is beneficial.** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

42. **4. Following the organization's ICT Security Policy is useful.** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Normative Belief

Please indicate the number that best matches the degree to which you agree or disagree with the statements (where 1-Strongly disagree, and 5-Strongly agree).

43. **5. My managers thinks that I should follow the organization's ICT Security Policy.** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

44. **6. My executives think that I should follow the organization's ICT Security Policy.** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

45. **7. My colleagues think I should follow the organization's ICT Security Policy.** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Self-Efficacy

Please indicate the number that best match your judgement for the following statements (where 1- Almost never, and 5- Almost always).

46. **8. I have the necessary skills to fulfill the requirements of the ICT Security Policy.** *

Mark only one oval.

	1	2	3	4	5	
Almost never	◯	◯	◯	◯	◯	Almost always

47. **9. I have the necessary knowledge to fulfill the requirements of the ICT Security Policy.** *

Mark only one oval.

	1	2	3	4	5	
Almost never	◯	◯	◯	◯	◯	Almost always

48. **10. I have the necessary competencies to fulfill the requirements of the ICT Security Policy.** *

Mark only one oval.

	1	2	3	4	5	
Almost never	◯	◯	◯	◯	◯	Almost always

SECTION D: INTENTION TO COMPLY WITH ICT SECURITY POLICY

In this section, the researcher is interested to assess employee's ICT Security Policy Compliance Intention. Please indicate the number that best matches the degree to which you agree or disagree with the statements (where 1- Strongly disagree, and 7- Strongly agree).

49. **1. It is my intention to continue to comply with the organization's ICT Security Policy.** *

Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

50. **2. I am certain I will adhere to my organization's ICT Security Policy.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

51. **3. I would follow the organization's ICT Security Policy whenever possible.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

52. **4. I am likely to follow the organization's ICT Security Policy in the future.** *
Mark only one oval.

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

SECTION E: SOCIAL DESIRABILITY

Listed below are a few statements related with personal attitudes and traits. Please indicate the number that best matches the degree of agreement or disagreement with each of the following statements that clearly correspond to your personal traits (where 1- Strongly disagree, and 5- Strongly agree).

53. **1. I like to gossip at times.**
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

54. **2. There have been occasions when I took advantage of someone.**
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

55. **3. I am always willing to admit it when I make a mistake.**
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

56. **4. I sometimes try to get my revenge rather than forgive and forget.**
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

57. **5. At times I have really insisted on having things my own way.**
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

58. **6. I have never been irked (irritated, inconvenienced, disturbed) when people expressed ideas very different from my own.**
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

59. **7. I have never deliberately (willfully, consciously) said something that hurt someone's feelings.**
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Powered by Google Forms

APPENDIX H
CROSS-LOADINGS (BEFORE REMOVING RM3 ITEM)

	PCM	RM	SETA	TMC	MON	ISK	ISKS	ATT	NB	SE	INT
PCM1	**0.786**	0.430	0.406	0.385	0.334	0.371	0.352	0.228	0.339	0.228	0.343
PCM2	**0.899**	0.560	0.506	0.503	0.388	0.493	0.432	0.367	0.384	0.262	0.424
PCM3	**0.895**	0.518	0.555	0.495	0.437	0.502	0.454	0.300	0.343	0.277	0.355
PCM4	**0.845**	0.504	0.501	0.506	0.395	0.473	0.404	0.269	0.326	0.242	0.356
RM1	0.546	**0.866**	0.512	0.589	0.484	0.622	0.461	0.352	0.346	0.205	0.424
RM2	0.485	**0.899**	0.532	0.591	0.552	0.655	0.491	0.301	0.352	0.196	0.424
RM3	0.442	**0.699**	0.311	0.439	0.346	0.416	0.432	0.435	0.335	0.177	0.526
RM4	0.510	**0.886**	0.609	0.668	0.547	0.687	0.490	0.329	0.387	0.264	0.425
SETA1	0.524	0.514	**0.885**	0.648	0.544	0.636	0.490	0.239	0.398	0.313	0.318
SETA2	0.551	0.513	**0.903**	0.650	0.554	0.614	0.483	0.229	0.416	0.301	0.316
SETA3	0.456	0.523	**0.874**	0.675	0.493	0.652	0.505	0.218	0.345	0.330	0.283
SETA4	0.514	0.562	**0.885**	0.706	0.497	0.686	0.539	0.241	0.395	0.318	0.327
TMC1	0.526	0.602	0.746	**0.909**	0.535	0.686	0.585	0.350	0.477	0.298	0.431
TMC2	0.532	0.660	0.720	**0.960**	0.587	0.744	0.617	0.403	0.480	0.298	0.462
TMC3	0.515	0.660	0.702	**0.956**	0.587	0.743	0.576	0.400	0.469	0.296	0.454
TMC4	0.492	0.638	0.650	**0.903**	0.552	0.685	0.554	0.401	0.487	0.237	0.483
MON1	0.423	0.540	0.579	0.584	**0.855**	0.601	0.505	0.233	0.349	0.215	0.278
MON2	0.410	0.547	0.526	0.582	**0.886**	0.620	0.451	0.289	0.370	0.210	0.326
MON3	0.394	0.486	0.488	0.491	**0.910**	0.569	0.438	0.190	0.281	0.206	0.247
MON4	0.390	0.491	0.497	0.495	**0.908**	0.608	0.473	0.213	0.313	0.250	0.255
ISK1	0.444	0.630	0.586	0.623	0.568	**0.862**	0.511	0.327	0.389	0.269	0.378
ISK2	0.487	0.697	0.629	0.729	0.649	**0.910**	0.567	0.366	0.457	0.293	0.434
ISK3	0.458	0.671	0.590	0.688	0.593	**0.884**	0.514	0.377	0.439	0.261	0.431
ISK4	0.485	0.591	0.706	0.669	0.592	**0.902**	0.589	0.302	0.474	0.379	0.368
ISK5	0.522	0.603	0.728	0.695	0.595	**0.886**	0.602	0.309	0.456	0.383	0.370
ISKS1	0.434	0.439	0.589	0.543	0.483	0.572	**0.829**	0.219	0.370	0.416	0.284
ISKS2	0.407	0.447	0.551	0.539	0.490	0.572	**0.837**	0.216	0.375	0.428	0.282

Cross-Loading (Before Removing RM3 Item) continued

	PCM	RM	SETA	TMC	MON	ISK	ISKS	ATT	NB	SE	INT

ISKS3	0.409	0.470	0.466	0.515	0.428	0.521	**0.895**	0.350	0.414	0.341	0.430
ISKS4	0.414	0.506	0.422	0.532	0.420	0.504	**0.859**	0.412	0.424	0.292	0.526
ISKS5	0.350	0.478	0.342	0.497	0.378	0.458	**0.778**	0.473	0.422	0.232	0.538
ATT1	0.317	0.375	0.245	0.397	0.259	0.352	0.392	**0.930**	0.491	0.226	0.556
ATT2	0.292	0.349	0.226	0.374	0.237	0.344	0.333	**0.919**	0.487	0.204	0.553
ATT3	0.343	0.410	0.261	0.396	0.241	0.366	0.377	**0.955**	0.510	0.247	0.569
ATT4	0.332	0.408	0.251	0.398	0.242	0.359	0.367	**0.952**	0.499	0.230	0.562
NB1	0.409	0.431	0.411	0.500	0.356	0.497	0.459	0.537	**0.968**	0.339	0.514
NB2	0.390	0.404	0.406	0.484	0.359	0.478	0.445	0.515	**0.972**	0.341	0.507
NB3	0.363	0.370	0.442	0.485	0.346	0.456	0.461	0.463	**0.926**	0.347	0.481
SE1	0.275	0.226	0.344	0.284	0.251	0.332	0.394	0.223	0.333	**0.966**	0.356
SE2	0.300	0.258	0.352	0.310	0.240	0.369	0.408	0.245	0.354	**0.975**	0.386
SE3	0.283	0.248	0.340	0.287	0.229	0.338	0.393	0.233	0.354	**0.969**	0.362
INT1	0.419	0.507	0.367	0.487	0.309	0.449	0.491	0.591	0.524	0.382	**0.947**
INT2	0.408	0.513	0.353	0.479	0.308	0.446	0.472	0.539	0.495	0.404	**0.944**
INT3	0.419	0.493	0.316	0.451	0.285	0.399	0.439	0.564	0.482	0.327	**0.963**
INT4	0.398	0.485	0.301	0.451	0.286	0.403	0.443	0.578	0.496	0.333	**0.959**

APPENDIX I
CROSS-LOADINGS (AFTER REMOVING RM3 ITEM)

	PCM	RM	SETA	TMC	MON	ISK	ISKS	ATT	NB	SE	INT
PCM1	**0.785**	0.415	0.406	0.385	0.334	0.371	0.352	0.228	0.339	0.228	0.343
PCM2	**0.899**	0.534	0.506	0.503	0.388	0.493	0.432	0.367	0.384	0.262	0.424
PCM3	**0.896**	0.504	0.555	0.495	0.437	0.502	0.454	0.300	0.343	0.277	0.355
PCM4	**0.845**	0.493	0.501	0.506	0.395	0.473	0.404	0.269	0.326	0.242	0.356
RM1	0.546	**0.887**	0.512	0.589	0.484	0.622	0.460	0.352	0.346	0.205	0.424
RM2	0.485	**0.914**	0.532	0.591	0.552	0.655	0.491	0.301	0.352	0.196	0.424
RM4	0.510	**0.902**	0.609	0.668	0.547	0.687	0.490	0.329	0.387	0.264	0.425
SETA1	0.524	0.538	**0.885**	0.648	0.544	0.637	0.491	0.239	0.399	0.313	0.318
SETA2	0.551	0.531	**0.903**	0.650	0.554	0.614	0.483	0.229	0.416	0.301	0.316
SETA3	0.456	0.539	**0.873**	0.675	0.493	0.652	0.506	0.218	0.346	0.330	0.283
SETA4	0.514	0.566	**0.884**	0.706	0.497	0.686	0.539	0.241	0.395	0.318	0.327
TMC1	0.527	0.604	0.746	**0.909**	0.535	0.686	0.585	0.350	0.477	0.298	0.431
TMC2	0.532	0.666	0.720	**0.960**	0.587	0.744	0.617	0.403	0.480	0.298	0.462
TMC3	0.515	0.661	0.702	**0.956**	0.587	0.743	0.576	0.400	0.469	0.296	0.454
TMC4	0.492	0.622	0.650	**0.903**	0.552	0.685	0.554	0.401	0.487	0.237	0.483
MON1	0.423	0.543	0.579	0.584	**0.855**	0.601	0.506	0.233	0.349	0.215	0.278
MON2	0.410	0.545	0.526	0.582	**0.886**	0.620	0.451	0.289	0.370	0.210	0.326
MON3	0.394	0.493	0.488	0.491	**0.910**	0.569	0.438	0.190	0.281	0.206	0.247
MON4	0.390	0.501	0.497	0.495	**0.909**	0.608	0.473	0.213	0.313	0.250	0.255
ISK1	0.444	0.640	0.586	0.623	0.568	**0.862**	0.511	0.327	0.389	0.269	0.378
ISK2	0.487	0.702	0.629	0.729	0.649	**0.910**	0.567	0.366	0.457	0.293	0.434
ISK3	0.458	0.666	0.590	0.688	0.593	**0.883**	0.514	0.377	0.439	0.261	0.431
ISK4	0.485	0.609	0.706	0.669	0.592	**0.902**	0.590	0.302	0.474	0.379	0.368
ISK5	0.522	0.617	0.728	0.695	0.595	**0.886**	0.603	0.309	0.456	0.383	0.370
ISKS1	0.434	0.438	0.589	0.543	0.483	0.572	**0.831**	0.219	0.370	0.416	0.284
ISKS2	0.407	0.453	0.551	0.539	0.490	0.572	**0.838**	0.216	0.375	0.428	0.282
ISKS3	0.409	0.448	0.466	0.515	0.428	0.521	**0.894**	0.350	0.414	0.341	0.430

Cross-Loading (After Removing RM3 Item) continued

	PCM	RM	SETA	TMC	MON	ISK	ISKS	ATT	NB	SE	INT

ISKS4	0.414	0.472	0.422	0.532	0.420	0.503	**0.858**	0.412	0.424	0.292	0.526
ISKS5	0.350	0.433	0.342	0.496	0.378	0.457	**0.777**	0.473	0.422	0.232	0.538
ATT1	0.317	0.326	0.245	0.397	0.259	0.351	0.391	**0.930**	0.491	0.226	0.556
ATT2	0.292	0.302	0.226	0.374	0.237	0.344	0.333	**0.919**	0.487	0.204	0.553
ATT3	0.343	0.365	0.261	0.396	0.241	0.366	0.377	**0.955**	0.510	0.247	0.569
ATT4	0.332	0.370	0.251	0.398	0.242	0.359	0.366	**0.952**	0.499	0.230	0.562
NB1	0.409	0.411	0.411	0.500	0.356	0.497	0.458	0.537	**0.967**	0.339	0.514
NB2	0.390	0.388	0.406	0.484	0.359	0.478	0.445	0.515	**0.972**	0.341	0.507
NB3	0.363	0.352	0.442	0.485	0.346	0.456	0.460	0.463	**0.926**	0.347	0.481
SE1	0.275	0.222	0.344	0.284	0.251	0.332	0.394	0.223	0.333	**0.966**	0.356
SE2	0.300	0.252	0.352	0.310	0.240	0.369	0.409	0.245	0.354	**0.975**	0.386
SE3	0.283	0.244	0.340	0.287	0.229	0.338	0.394	0.233	0.354	**0.969**	0.362
INT1	0.419	0.449	0.367	0.487	0.309	0.449	0.490	0.591	0.524	0.382	**0.947**
INT2	0.408	0.472	0.353	0.479	0.308	0.446	0.471	0.539	0.495	0.404	**0.944**
INT3	0.419	0.439	0.316	0.451	0.285	0.399	0.438	0.564	0.482	0.327	**0.963**
INT4	0.398	0.436	0.301	0.451	0.286	0.403	0.442	0.578	0.496	0.333	**0.959**