INFORMATION SECURITY POLICY COMPLIANCE BEHAVIOUR MODEL FOR MALAYSIAN FEDERAL PUBLIC SECTOR AGENCIES

PUSPADEVI A/P KUPPUSAMY

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia

AUGUST 202

DEDICATION

This thesis is dedicated to my husband (Mr.Sivabalan) and kids (Vihaan &Vidhyan)

ACKNOWLEDGEMENT

First and foremost, I am extremely grateful to my main supervisor, Dr. Ganthan Narayanasamy and co-supervisor Dr. Nurazean Binti Maarop for their invaluable advice, and continuous support during my PhD study. I am also grateful to be able to learn about research development and analysis from academicians such as Prof. Dr. T.Ramayah and seniors such as Dr. Azlina Abdul Aziz. I would like to express my gratitude to all the experts involved and respondents participated in this study.

Most importantly, I would like to express my utmost gratitude to my husband Mr.Sivabalan, awesome kids Vihaan and Vidhyan, my parents Mr.&Mrs. Kuppusamy Kamala, my parents in-law Mr.Mrs.Seenivasakam Valiammah, my siblings, aunty lalitha, family members and my kid's babysitters for the support throughout this PhD Journey. Thank you to my hubby for the incredible understanding, immense encouragement, infinite love. Thank you to my little superheroes for being awesome, understanding, and great kids.

Thank you so much Valli Krishnan akka for being there to take care of my kids in time of needs. Really appreciated it akka. Finaly, thank you to everyone who made it possible for me to complete this study.

ABSTRACT

Organizations leverage information security policies (ISP) to prevent information security incidents, but employees often fail to comply with them. As such, the Malaysian public sector has a comprehensive ISP in the form of circulars, policies, procedures, frameworks, and strategic plans. However, ISP compliance among Malaysian public sector employees remains low, with limited studies found in extant research. Hence, this research aims to develop and validate a new model of factors that influence ISP compliance behaviour among Malaysian federal public sector agency employees. The research started with the identification of problems through conducting interviews with the relevant agencies and knowledge gaps by reviewing existing ISP literature. Then, a systematic literature review (SLR) was performed and analysed to identify the influencing factors of ISP compliance behaviour. A conceptual model was developed using factors from the theory of planned behaviour, social bond theory, protection motivation theory, and several other factors from literatures. Next, the survey instrument items were developed, their content validated by nine experts, and a pilot test was conducted with 30 respondents. Subsequently, data collection was conducted through email among 27 federal agency employees in Putrajaya and Kuala Lumpur, Malaysia. As a result, 360 valid responses were analysed to validate the conceptual model using ‘partial least square-structured equation modelling’ analysis. The model validation revealed that ‘attitude’, ‘perceived behavioural control’, ‘perceived response efficacy’, ‘perceived punishment severity’, ‘attachment’, ‘commitment’, ‘belief’, and ‘perceived benefit’ have positive effects on ISP compliance intention with p-value < 0.05. However, five factors, namely ‘subjective norm’, ‘threat severity’, ‘threat vulnerability’, ‘awareness training’ and ‘involvement’ were found to be non-significant towards ISP compliance intention with p-value > 0.05. These research findings were used to develop ISP compliance guidelines for the Malaysian public sector. The ISP compliance guidelines were reviewed by three ISP practitioners. Overall, this research contributes theoretically, contextually, and practically towards ISP compliance, especially in the context of the Malaysian federal public sector agencies.

ABSTRAK

Organisasi memanfaatkan dasar keselamatan maklumat (ISP) untuk mencegah insiden keselamatan maklumat, tetapi pekerja sering gagal mematuhinya. Oleh yang demikian, sektor awam Malaysia mempunyai ISP yang komprehensif dalam bentuk pekeliling, dasar, prosedur, rangka kerja dan pelan strategik. Walau bagaimanapun, pematuhan ISP dalam kalangan kakitangan sektor awam Malaysia kekal rendah, dan kajian lepas dalam penyelidikan ini adalah terhad. Oleh itu, kajian ini bertujuan untuk membangunkan dan mengesahkan model baharu bagi faktor-faktor yang mempengaruhi tingkah laku pematuhan ISP dalam kalangan kakitangan agensi sektor awam persekutuan Malaysia. Kajian dimulakan dengan mengenal pasti masalah melalui temu bual dengan agensi berkaitan dan jurang pengetahuan dengan mengkaji kajian lepas yang sedia ada. Kemudian, kajian literatur sistematik (SLR) dilakukan dan dianalisis untuk mengenal pasti faktor-faktor yang mempengaruhi tingkah laku pematuhan ISP. Model konseptual dibangunkan menggunakan faktor-faktor daripada teori tingkah laku terancang, teori ikatan sosial, teori motivasi perlindungan dan beberapa faktor lain daripada kajian lepas. Seterusnya, item instrumen soal selidik telah dibangunkan, kandungannya disahkan oleh sembilan pakar, serta ujian rintis telah dijalankan dengan 30 responden. Selepas itu, pengumpulan data telah dijalankan menerusi e-mel dalam kalangan kakitangan di 27 agensi persekutuan di Putrajaya dan Kuala Lumpur, Malaysia. Sebanyak 360 respons yang sah telah dianalisis untuk mengesahkan model konseptual menggunakan analisis ‘pemodelan persamaan berstruktur separa terkecil’. Pengesahan model mendedahkan bahawa ‘sikap’, ‘kawalan tingkah laku yang dirasakan’, ‘keberkesanan tindak balas’, ‘keterukan hukuman’, ‘keterikatan’, ‘komitmen’, ‘kepercayaan’, dan ‘faedah yang dirasakan’ mempunyai kesan positif terhadap niat pematuhan ISP dengan nilai-p < 0.05. Bagaimanapun, lima faktor iaitu ‘norma subjektif’, ‘keterukan ancaman’, ‘kelemahan ancaman’, ‘latihan kesedaran’ dan ‘penglibatan’ didapati tidak signifikan terhadap niat pematuhan ISP dengan nilai-p > 0.05. Hasil kajian ini digunakan untuk membangunkan garis panduan pematuhan ISP untuk sektor awam Malaysia. Garis panduan pematuhan ISP telah disemak oleh tiga pengamal ISP. Secara keseluruhannya, kajian ini menyumbang secara teori, kontekstual dan praktikal ke arah pematuhan ISP, terutamanya dalam konteks agensi sektor awam persekutuan Malaysia.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

SDT	-	Self Determination Theory
DT	-	Deterrence Theory
PMT	-	Protection Motivation Theory
TPB	-	Theory of Planned behaviour
SBT	-	Social Bond Theory
RCT	-	Rational Choice Theory
HBM	-	Health Belief Model
ISC	-	Information Security Compliance
JD-R	-	Extended Job Demands-Resources
EPPM	-	Extended Parallel Processing Model
TIB	-	Theory of Interpersonal Behaviour
ISP	-	Information Security Policy
TRA	-	Theory of Reasoned Action
RAKKSSA	-	Public Sector Cyber Security Framework
ICT	-	Information Communication Technology
CERT	-	Computer Emergency Response Team
ISMS	-	Information Security Management System
BCM	-	Business Continuity Management
GCERT	-	Government Computer Emergency Response Team
PLS-SEM	-	Partial Least Squares Structural Equation Modelling
IPMA	-	Importance and Performance Matrix Analysis
CMV	-	Common Method Variance
CVI	-	Content Validity Index
CVR	-	Content Validity Ratio
VIF	-	Variance Inflation Factors
AVE	-	Average Variance Extracted

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Organisations reliance on information technology have increased tremendously and brought many advantages. The prevalent use of information technology has resulted in an exponential increase in information security threats and attacks (Humayun, Niazi, Jhanjhi, Alshayeb, & Mahmood, 2020). Therefore, information security becomes a necessity for organizations. Globally, information security becoming top priority as worldwide threat assessment of the United States intelligence community put cyber threat as the top priority ahead of other prominent threats including weapons of mass destruction and proliferation, terrorism, and counter intelligence (CIA, 2019). Meanwhile Malaysia's cybersecurity strategy for 2020-2024 recognizes information security as a vital national priority (National Security Council, 2019). According to the report, government now has to deal with cyber threats from state sponsored actors aimed at critical targets of national importance.

At the outset, a lot of initiatives taken to address information security threats in technological context but later discovered that it is not sufficient to guarantee overall information security in organisations (Ifinedo, 2014; Kim, Yang, & Park, 2014; Metalidou et al., 2014; Safa, Solms, & Futcher, 2016; Soomro, Shah, & Ahmed, 2016). Growing security threats despite advanced technological solutions in place have extended researchers attention to explore on the human aspect such as employees behaviour in an organisation (Ifinedo, 2014; Metalidou et al., 2014; Safa et al., 2016).

First, employees need guidance to prevent, face and manage information security threats. Therefore, information security policy is developed to provide relevant guide and support to the employees within an organization with regard to information security (Sommestad, Karlzén, & Hallberg, 2015). Information security policy is defined as guidelines, requirements, and rules developed by management to guide employee's behaviours (Ifinedo, 2014). Information security policy generally include acceptable use of computer resources, accountabilities concerning information security and sometimes the consequences of security policy violation (Sommestad et al., 2015). Information security policy is responsible to secure information security of an organization if the anticipated behaviour mandated in policy is achieved by observance or compliance of the policy by employees (Kim et al., 2014; Sohrabi Safa, Von Solms, & Furnell, 2016; Sommestad et al., 2015). Therefore, information security policy compliance is one of the key challenges being faced by organisation around the globe.

Typically, organizations around the globe especially public sector do have comprehensive information security policy such specific cybersecurity framework by national institute of standards and technology (NIST) United States and basic policies such as a disaster recovery policy, data backup policy, or risk assessment policy and so on. Relatively Malaysian public sector does have a list of policies, framework, circulars, best practises, standard requirements, guidelines, instruction letters and security procedures in place (Section 2.3.1). These lists of documents are generalised and referred as 'information security policy (ISP)' are applicable to all Malaysian public sector employees. Malaysian public sector employees must know, understand and comply to ISP (MAMPU, 2016).

According to Malaysian national cybersecurity strategy 2020-2025 report employees remain a significant information security risk to organisation (National Security Council, 2019). According to that report, there were also incidents where these insiders (employees), unknowingly become victims of elaborated cybercrime schemes such as watering hole attacks, social engineering ploys, malware and ransomware infections, propagation mechanism by inserting infected universal serial bus (USB) devices into the internal networks or arbitrarily clicking on links found in emails or while browsing the internet (National Security Council, 2019). The report also stated that numerous cases of intellectual property theft and the leaking of sensitive information have caused substantial financial and reputational damage (National Security Council, 2019).

This chapter gives introduction and overview of this thesis. First, the chapter provide background of problem (section 1.2), second, it describes problem statement of the research (section 1.3). Third, it describes the research questions (section 1.4) and research objectives (section 1.5). Then, it continues to describe research scope (section 1.6), significance of the research (Section 1.7) and finally, structure of the thesis content (Section 1.8).

1.2 Background of Problem

ISP which includes mandatory organisational rules, policies, frameworks, procedure, guidelines, requirements and best practices essential to control employees security behaviours in cyber environment (Bauer & Bernroider, 2017; Ifinedo, 2018). ISP compliance ensure adherence to safe practise by employees. Employees should comply to these policies to defend their organisation's resources and assets (Lowry & Moody, 2015; Yazdanmehr & Wang, 2016). Having ISP is in place does not guarantee that employees will comply to its specifications (Ifinedo, 2018). In reality, employees noncompliance to ISP, leads to greater information security complications such as information security incidents (Han, Kim, & Kim, 2017; Siponen, Adam Mahmood, & Pahnila, 2014).

Although various ISP have been developed and deployed, the employee's compliance to ISP remains low (D'Arcy & Lowry, 2017; Ifinedo, 2018; Chenhui Liu, Wang, & Liang, 2020). Employees tend to ignore ISP which leads to incidents of unsafe security activities, such as downloading unverified software from the internet, using simple and obvious passwords and sharing computer accounts (Pham, El-Den, & Richardson, 2016). Such unsafe security behaviour have the potential to compromise the organisation security system, despite having the best ISP (Pham et al., 2016). Hence, employees causes breaches to information resources and assets of organisations (Lowry & Moody, 2015).

Employees has been described as the critical factor and weakest link in an organisation (Ifinedo, 2014; Stewart & Jurjens, 2017). Employees does not comply to

ISP for many reasons including unawareness of ISP, carelessness, laziness, mischief, and conflict (Lowry & Moody, 2015; Siponen et al., 2014; Sohrabi Safa et al., 2016). Sometimes, employees may find complying to ISP is time consuming and inconvenient, as it has the potential to obstruct their daily routine work (Pham et al., 2016).

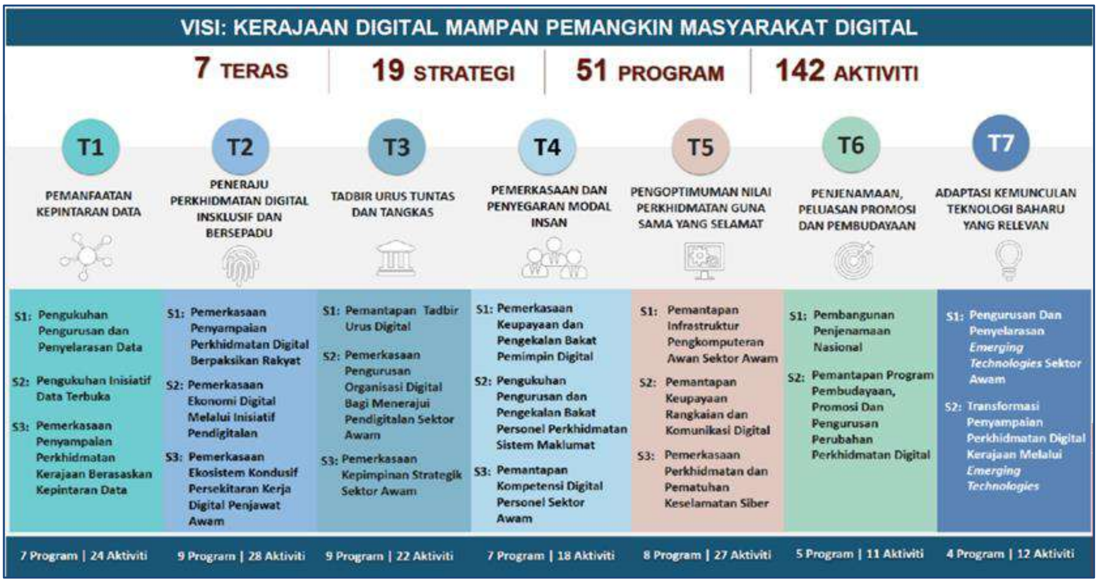
A number of 10,790 security incidents have been recorded in Malaysia involving spam, intrusion attempt, denial of service, fraud, malicious code, content related incidents, intrusion, cyber harassment and vulnerability report meanwhile malware infection and botnet drones accumulated to 5,508,357 devices in the year 2020 (MYCERT, 2020). As for year 2021, a number of 10,016 security incidents and 2,746,265 malware and botnet infected devices was reported (MyCERT, 2014). Meanwhile, Malaysian public sector security incidents statistics from year 2015 up until 31 July 2021 is shown in Table 1.1. It is important to note that most of Malaysian public sector employees was working from home (WFH) during 2020 and 2021 and any security incidents that happen in employees home network is not covered. Hence, the actual number of incidents are far more than the reported cases.

Table 1.1 Cyber security incidents of Malaysian public sector (Cybersecurity, 2021)

	2021*	**2020**	**2019**	**2018**	**2017**	**2016**	**2015**
Content related	2	5	14	8	2	0	0
Cyber harassment	0	2	1	1	0	1	0
DoS	1	1	0	1	0	0	2
Fraud	4	11	4	16	7	17	10
Intrusion	29	66	63	49	36	122	75
Intrusion attempt	0	0	0	0	0	1	4
Malicious codes	2	6	4	6	16	13	13
Spam	1	6	4	3	4	3	1
Vulnerabilities report	5	8	13	43	13	7	3
Total	**44**	**105**	**103**	**127**	**78**	**164**	**108**

***until 31st July 2021**

Every employee in Malaysian public sector is subject to complying with ISP, hence they should equip themselves with an understanding of information security risks and know the relevant preventive measures, take responsibility, and take steps to improve information security. Noncompliance among Malaysian public sector employees to ISP have huge impact where it erodes the public's trust in the governance of Malaysian public sector organizations to protect their information assets. Hence the urgency in identifying solution in improving the ISP compliance behaviour among Malaysian public sector employees expressed in Public Sector Digitization Strategic Plan (PSPSA) 2021-2025 (MAMPU, 2021). As of Figure 1.1, under strategic thrust 5 which is ‘optimization of equalized service value’, outlined the strategy 3 which is ‘strengthening service and cyber security compliance’. This is also in line with the sustainable development goals 2030 (SDG 2030) of United Nation, the 12th Malaysia plan (RMKe-12) and the aspirations of the vision for common prosperity 2030 (WKB 2030).



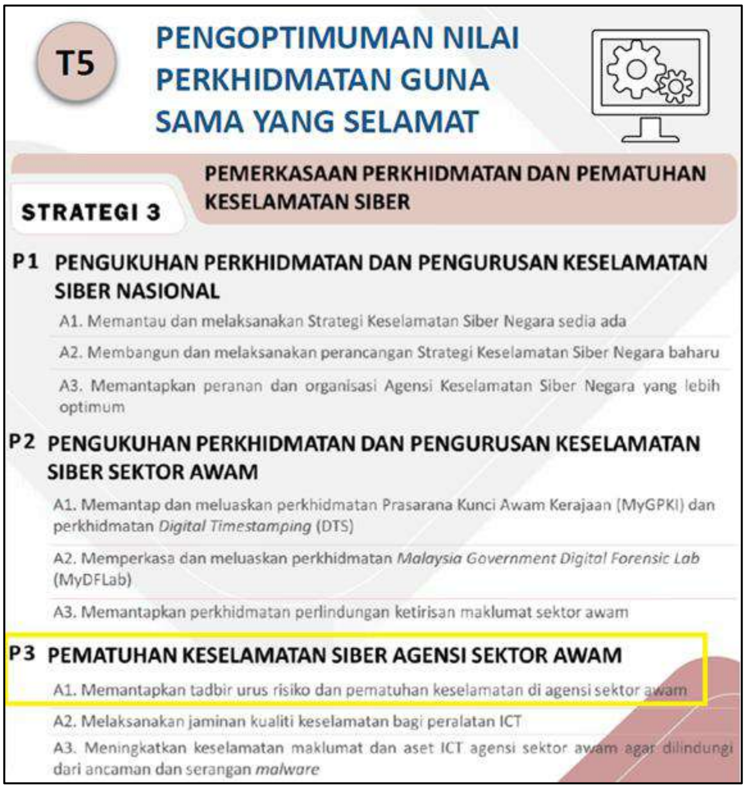
VISI: KERAJAAN DIGITAL MAMPAN PEMANGKIN MASYARAKAT DIGITAL

7 TERAS | 19 STRATEGI | 51 PROGRAM | 142 AKTIVITI

T1	T2	T3	T4	T5	T6	T7
PEMANFAATAN KEPINTARAN DATA	PENERAJU PERKHIDMATAN DIGITAL INSKLUSIF DAN BERSEPADU	TADBIR URUS TUNTAS DAN TANGKAS	PEMERKASAAN DAN PENYEGARAN MODAL INSAN	PENGOPTIMUMAN NILAI PERKHIDMATAN GUNA SAMA YANG SELAMAT	PENJENAMAAN, PELUASAN PROMOSI DAN PEMBUDAYAAN	ADAPTASI KEMUNCULAN TEKNOLOGI BAHARU YANG RELEVAN
S1: Pengukuhan Pengurusan dan Penyelarasan Data	S1: Pemerkasaan Penyampaian Perkhidmatan Digital Berpaksikan Rakyat	S1: Pemantapan Tadbir Urus Digital	S1: Pemerkasaan Keupayaan dan Pengekalan Bakat Pemimpin Digital	S1: Pemantapan Infrastruktur Pengkomputeran Awan Sektor Awam	S1: Pembangunan Penjenamaan Nasional	S1: Pengurusan Dan Penyelarasan *Emerging Technologies* Sektor Awam
S2: Pengukuhan Inisiatif Data Terbuka	S2: Pemerkasaan Ekonomi Digital Melalui Inisiatif Pendigitalan	S2: Pemerkasaan Pengurusan Organisasi Digital Bagi Menerajui Pendigitalan Sektor Awam	S2: Pengukuhan Pengurusan dan Pengekalan Bakat Personel Perkhidmatan Sistem Maklumat	S2: Pemantapan Keupayaan Rangkaian dan Komunikasi Digital	S2: Pemantapan Program Pembudayaan, Promosi Dan Pengurusan Perubahan Perkhidmatan Digital	S2: Transformasi Penyampaian Perkhidmatan Digital Kerajaan Melalui *Emerging Technologies*
S3: Pemerkasaan Penyampaian Perkhidmatan Kerajaan Berasaskan Kepintaran Data	S3: Pemerkasaan Ekosistem Kondusif Persekitaran Kerja Digital Penjawat Awam	S3: Pemerkasaan Kepimpinan Strategik Sektor Awam	S3: Pemantapan Kompetensi Digital Personel Sektor Awam	S3: Pemerkasaan Perkhidmatan dan Pematuhan Keselamatan Siber		
7 Program | 24 Aktiviti	9 Program | 28 Aktiviti	9 Program | 22 Aktiviti	7 Program | 18 Aktiviti	8 Program | 27 Aktiviti	5 Program | 11 Aktiviti	4 Program | 12 Aktiviti

Figure 1.1 Trust and strategy outlined in PSPSA 2021-2025 (MAMPU, 2021)

PSPSA have regarded ISP compliance as vital through implementation plan to strengthen cyber security compliance among public sector agencies as in Figure 1.2.



T5 PENGOPTIMUMAN NILAI PERKHIDMATAN GUNA SAMA YANG SELAMAT

STRATEGI 3 PEMERKASAAN PERKHIDMATAN DAN PEMATUHAN KESELAMATAN SIBER

P1 PENGUKUHAN PERKHIDMATAN DAN PENGURUSAN KESELAMATAN SIBER NASIONAL

A1. Memantau dan melaksanakan Strategi Keselamatan Siber Negara sedia ada

A2. Membangun dan melaksanakan perancangan Strategi Keselamatan Siber Negara baharu

A3. Memantapkan peranan dan organisasi Agensi Keselamatan Siber Negara yang lebih optimum

P2 PENGUKUHAN PERKHIDMATAN DAN PENGURUSAN KESELAMATAN SIBER SEKTOR AWAM

A1. Memantap dan meluaskan perkhidmatan Prasarana Kunci Awam Kerajaan (MyGPKI) dan perkhidmatan *Digital Timestamping* (DTS)

A2. Memperkasa dan meluaskan perkhidmatan *Malaysia Government Digital Forensic Lab* (MyDFLab)

A3. Memantapkan perkhidmatan perlindungan ketirisan maklumat sektor awam

P3 PEMATUHAN KESELAMATAN SIBER AGENSI SEKTOR AWAM

A1. Memantapkan tadbir urus risiko dan pematuhan keselamatan di agensi sektor awam

A2. Melaksanakan jaminan kualiti keselamatan bagi peralatan ICT

A3. Meningkatkan keselamatan maklumat dan aset ICT agensi sektor awam agar dilindungi dari ancaman dan serangan *malware*

Figure 1.2 Information security compliance of public sector agencies (under T5, Strategi 3 and P3) in PSPSA (MAMPU, 2021)

Numerous programs are in place to encourage ISP compliance behaviour among Malaysia public sector employees, but the full impact of the activities and programs under the strategy mentioned in Figure 1.2 has not been quantified. Therefore, the central problem researched by this study is the low ISP compliance behaviour among Malaysian public sector employees which resulted in security breaches. A preliminary interview involving three (3) main agencies coordinating cybersecurity in Malaysia, namely National Cyber Security Agency (NACSA), Cybersecurity Malaysia (CSM) and Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) was conducted and found ISP compliance behaviour among Malaysian public sector employees is low (Section 3.3.1). This is an area of increasing concern as it impacts public trust, national sovereignty, national security and also public service delivery (Dzazali & Zolait, 2012; Teoh, Mahmood, & Dzazali, 2018). A case study conducted through qualitative approach using semi-structured interviews on cyber security challenges in Malaysian public sector organisations also revealed that, despite being weakest link, Malaysian public sector employees are not been able to address successfully in term of cybersecurity (Teoh et al., 2018). Further research in this area is needed to uncover what factor contribute to ISP compliance intention among Malaysian public sector employees since Malaysian public sector employee's compliance to ISP is relatively not examined before.

1.3 Problem Statement

A rationale to this research aim is based on the low ISP compliance behaviour among Malaysian public sector employees which was confirmed during the interview and knowledge gap analyses of the extant research as described in section 2.8. The gap analyses advocate the development of new ISP compliance behaviour model in sixfold problem which are 'lack of ISP compliance model for Malaysian public sector', 'lack of generalizability', 'lack of studies about social bonding perspective on attitude towards intention to comply to ISP', 'no study that explores the integration of theory of planned behaviour (TPB), social bond theory (SBT), protection motivation theory (PMT) and other significant factors to form ISP compliance model', 'lack of studies that examine the relationship between perceived benefit and attitude', and 'lack of ISP compliance guidelines for the public sector especially in Malaysia'. Hence, this research aims to develop, validate, and evaluate a new model of the behavioural factors that influence the ISP compliance intention among Malaysian public sector employees in the attempts to address the low ISP compliance problem and knowledge gaps.

1.4 Research Questions

The main questions of this research are as below: -

(a) What are the factors that influence information security policy compliance behaviour among Malaysian public sector employees?

(b) How to develop information security policy compliance behaviour model for Malaysian public sector employees?

(c) How to validate the information security policy compliance behaviour model for Malaysian public sector employees?

(d) What are the relevant guidelines can be proposed based on model findings for Malaysian public sector employees?

1.5 Research Objective

To answer the formulated research questions, four research objectives were constructed. Those research objectives were defined to achieve the aim of this research which to develop, validate a new model of factors that influence the ISP compliance intention among Malaysian public sector employees and help to increase their ISP compliance. The research objectives are as below: -

(a) To identify factors that influence information security policy compliance behaviour among Malaysian public sector employees.

(b) To develop a new information security policy compliance behaviour model for Malaysian public sector employees.

(c) To validate the new information security policy compliance behaviour model for Malaysian public sector employees.

(d) To propose appropriate ISP compliance guidelines for Malaysian public sector employees based on proposed model findings.

1.6 Scope of study

The scope of this research is categorised into five main perspectives which are ISP compliance stage, ISP compliance study, level of analysis, ISP cluster, and respondents. Table 1.2 indicates the perspectives, types and scope applied in this research.

Table 1.2 Scope of the research

Perspective	**Type**	**Scope of this research**
ISP compliance behaviour stage	i. Intention to comply ii. Actual compliance	Intention to comply
ISP compliance behaviour study	i. Relational ii. Descriptive iii. Comparative	Relational
Level of analysis	i. Individual ii. Organization	Individual (Employee)
Cluster	i. Telecommunication ii. Education iii. Health iv. Others (etc)	Public Sector of Malaysia
Respondents	Malaysian public sector employees	Employees of Malaysian federal public sector agencies

The dependant variable in this research is the 'intention to comply' measuring Malaysian public sector employee's intention to comply to ISP. Generally, ISP compliance stages can be categorised into two stages which are intention to comply (pre-compliance) and actual compliance (post-compliance). Intention to comply refers to the initial decision of the employee to comply to ISP. On the other hand, actual compliance refers to the willingness of the employee to continue complying to ISP. This research focuses on the intention to comply (pre-compliance) stage by Malaysian federal public sector employees. Studies can be classified into three main groups namely relational, descriptive, and comparative studies. This research applied relational study as it aims to investigate the relationship between the 14 independent factors obtained from the integration of TPB, SBT, PMT and past literatures, with dependant variable which is 'intention to comply' to ISP.

This research focuses on the ISP compliance intention from the perspective of Malaysian federal public sector employees at the individual level. Research conducted among employees from 27 federal agencies in Malaysian public sectors. The selection of agencies is based on suitability factors, involvement with the ISP and ease of obtaining feedback from respondents.

1.7 Significance of the study

This research is substantial from theoretical, contextual, and practical perspective. First, the development of a new ISP compliance behaviour model which consist of factors that influence ISP compliance intention among Malaysian federal Public sector employees has contributed to a new theoretical finding in ISP. It is done by incorporating the theory of TPB, SBT, PMT, and factors from prior studies to examine the influential factors of ISP compliance behaviour among Malaysian federal public sector employees. The findings implies that eight factors namely ‘attitude’, ‘perceived behavioural control’, ‘perceived response efficacy’, ‘perceived punishment severity’, ‘attachment’, ‘commitment’, ‘belief’ and ‘perceived benefit’ increase ISP compliance behaviour among Malaysian federal public sector employees. It is an effort to add new knowledge to the current research body by identifying factors that influence the ISP compliance behaviour, developing and proposing model to measure ISP compliance behaviour and propose strategic solutions for future improvement. The relationships between factors and ISP compliance behaviour intention are expected to contribute to the body of knowledge of ISP compliance.

As the TPB theory only defines the causal relationship between its own factors, this research extends the relationship by examining SBT factors into ‘attitude’ factor of TPB. This research reveals SBT factors such as ‘attachment’, ‘commitment’ and ‘belief’ has influenced ‘attitude’ factor towards ISP compliance intention. This relationship appears to be a new addition to knowledge by enriching the application of TPB. Moreover, the research also contributes to the knowledge by adding ‘perceived benefit’ from literature to influence ‘attitude’ besides SBT and the findings reveals it influence ‘attitude’ factor. Besides that, this research is strengthened with reduced bias because the data collection was conducted during movement control order (MCO) where most of the respondents works from home without direct pressure form top management and peer influence too.

Third, the findings of this research have valuable practical contribution. The involvement of cybersecurity practitioners in validating the survey instrument, and reviewing the proposed guidelines has made the research findings more reliable to be applied in real-world phenomena. In addition, this research also proposed ISP compliance guidelines for the Malaysian public sector based on proposed model findings (Appendix I) to increase the ISP compliance among Malaysian public sector employees. The proposed guidelines is timely since the intention of developing more ISP for Malaysian public sector has been established in Malaysian National Cybersecurity Strategy 2020-2025 and PSPSA 2021-2025.

In developing new ISP, the findings of this research would be beneficial for the ISP developer such as NACSA and MAMPU. ISP developers could understand the key constructs that must be considered for ISP compliance so that it can be widely accepted by public sector employees and other organizations too in the future. Findings can be used by the organisations to strategically plan to enhance their employee's ISP compliance behaviour to prevent security breaches. Overall, the model and guidelines developed from this research are expected to help in increasing Malaysian public sector employee's ISP compliance.

1.8 Structure of the thesis

This thesis is structured into six chapters. Chapter 1 is named introduction. This chapter discusses introduction, background, problem background, problem statement, research questions, research objectives, scope, and significance of the study. Chapter 2 is named literature review. Chapter 2 discusses the literature review, definition of key concepts by explaining the research key terms. Subsequently, review the related theories, describes systematic literature review that have been conducted in identifying related works within ISP compliance research area and influencing factor of ISP.

Chapter 2 also highlights knowledge gap in extant research to justify the rationale and novelty of this research.

Chapter 3 is named research methodology. This chapter discusses the research methodology which refers to the overall process involved in the research in fulfilling the research objectives and obtaining the expected deliverables. It starts with a discussion of research design, and research phases. Each phase of research design is explained in depth, and the outcomes are also presented. Chapter 4 is named conceptual model development. This chapter presents the process of the conceptual model development and content validation of the survey instruments.

Chapter 5 is named data analysis and findings and recommendation. This chapter presents the empirical data analysis and discussion in empirical findings of the research. First, initial preparation is described including response rate analysis, data cleaning, non-response bias test, common method bias test, and normality test. Second, descriptive analysis of the demographics is presented. Third, the measurement model analysis using Partial Least Squares Structural Equation Modelling (PLS-SEM) analysis is presented which includes internal consistency reliability, convergent validity, and discriminant validity. Fourth, the structural model analysis using PLS-SEM which includes collinearity, path coefficient, coefficient of determination, effect size, blindfolding and predictive relevance. Fifth, advanced PLS-SEM analysis such as importance and performance matrix analysis (IPMA) and PLSpredict was conducted and reported. Later, hypotheses testing was summarized and discussed in detail in Malaysian federal public sector employee's context. Eventually, this research proposes ISP compliance guidelines for Malaysian public sector. The guidelines development is also discussed in Chapter 5. Finally, Chapter 6 is named conclusion. It summarizes the research findings based on research objectives, research implications, limitations and recommended future work.

REFERENCES

Abdul Halim, H., Ahmad, N. H., Geare, A., & Thurasamy, R. (2019). Innovation culture in SMEs: The importance of organizational culture, organizational learning and market orientation. Entrepreneurship Research Journal, 9(3), 1–14. https://doi.org/10.1515/erj-2017-0014

Abed, J., & Weistroffer, H. R. (2016). Understanding deterrence theory in security compliance behavior : A quantitative meta- analysis approach. In Southern Association for Information Systems Conference.

Afthanorhan, A., Awang, Z., Abd Majid, N., Foziah, H., Ismail, I., Al Halbusi, H., & Tehseen, S. (2021). Gain more insight from common latent factor in structural equation modeling. In Journal of Physics: Conference Series (Vol. 1793, p. 12030). IOP Publishing.

Ahmad, Z., Ong, T. S., Liew, T. H., & Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees: An empirical analysis. Information and Computer Security, 27(2), 165–188. https://doi.org/10.1108/ICS-10-2017-0073

Ajzen, I. (1985). From intentions to actions: A Theory of planned behavior. In Action Control (pp. 11–39). https://doi.org/10.1007/978-3-642-69746-3_2

Al-Mukahal, H. M., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations. Information and Computer Security, 23(1), 102–118. https://doi.org/10.1108/ICS-03-2014-0018

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Information security policy compliance: The role of information security awareness. In Proceedings of the Eighteenth Americas Conference on Information Systems.

Al-Omari, A., El-Gayar, O., Deokar, A., & Walters, J. (2012). Information security policy compliance: An ethical perspective. In In Proceedings of the 6th Midwest Association for Information Systems Conference.

Alalwan, J. A. (2018). Fear of cybercrime and the compliance with information security policies: A theoretical study. In ACM International Conference Proceeding Series (pp. 85–87). https://doi.org/10.1145/3183586.3183590

Alanazi, S. T., Anbar, M., Ebad, S. A., Karuppayah, S., & Al-Ani, H. A. (2020). Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector. Symmetry, 12(9), 1–21. https://doi.org/10.3390/SYM12091544

Alaskar, M., Vodanovich, S., & Shen, K. N. (2015). Evolvement of information security research on employees' behavior: A systematic review and future direction. In Proceedings of the Annual Hawaii International Conference on System Sciences (Vol. 2015-March, pp. 4241–4250). https://doi.org/10.1109/HICSS.2015.508

Alec Cram, W., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. MIS Quarterly: Management Information Systems, 43(2), 525–554. https://doi.org/10.25300/MISQ/2019/15117

Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organizational governance, social bonds and information security policy compliance: A perspective towards oil and gas employees. Sustainability (Switzerland), 12(20), 1–27. https://doi.org/10.3390/su12208576

Alkalbani, A., Deng, H., & Kam, B. (2015). Investigating the role of socio-organizational factors in the information security compliance in organizations. In Australasian Conference on Information Systems. Retrieved from http://arxiv.org/abs/1606.00875

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information security compliance in organizations: What is so different about an institutional perspective. Data and Information Management, 1(2).

Allahyari, T., Hassanzadeh, R. N., Khosravi, Y., & Zayeri, F. (2011). Development and evaluation of a new questionnaire for rating of cognitive failures at work. International Journal of Occupational Hygiene.

Alotaibi, M., Furnell, S., & Clarke, N. (2017). Information security policies: A review of challenges and influencing factors. In 2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016 (pp. 352–358). https://doi.org/10.1109/ICITST.2016.7856729

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers and Security, 98. https://doi.org/10.1016/j.cose.2020.102003

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. Information & Computer Security, 26(4), 420–436. https://doi.org/10.1108/ICS-09-2017-0063

Amankwa, E., Loock, M., & Kritzinger, E. (2019). A Composite framework to promote information security policy compliance in organizations. In International Conference Europe Middle East & North Africa Information Systems and Technologies to Support Learning (pp. 458–468). Springer.

Ananthan, S. S., Manaf, H. A., Hidayati, M., & Dewi, D. S. K. (2019). The development of talent management in Malaysian public sector: A comprehensive review. Problems and Perspectives in Management, 17(2), 242–253. https://doi.org/10.21511/ppm.17(2).2019.18

Anderson, T., Curtis, A., & Wittig, C. (2014). Definition and theory in social innovation. Master of Arts in Social Innovation. Krems: Danube University.

Angraini, Alias, R. A., & Okfalisa. (2019). Information security policy compliance: Systematic literature review. In Procedia Computer Science (Vol. 161, pp. 1216–1224). Elsevier B.V. https://doi.org/10.1016/j.procs.2019.11.235

Astin, A. W. (2014). Student involvement: A developmental theory for higher education. College Student Development and Academic Life: Psychological, Intellectual, Social and Moral Issues, 251–263.

Babin, B. J., Griffin, M., & Hair, J. F. (2016). Heresies and sacred cows in scholarly marketing publications. Journal of Business Research, 69(8), 3133–3138. https://doi.org/10.1016/j.jbusres.2015.12.001

Bandura, A. (1989). Human agency in social cognitive theory. American Psychologist, 44(9), 1175–1184. https://doi.org/10.1037/0003-066X.44.9.1175

Bauer, S., & Bernroider, E. W. N. (2015). The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 9190, pp. 154–164). https://doi.org/10.1007/978-3-319-20376-8_14

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

Becker, G. S. (1974). A theory of social interactions. NBER Working Paper, 42(42), 1–54. https://doi.org/10.1086/260265

Becker, M. H. (1974). The health belief model and sick role behavior. Health Education Monographs, 2(4), 409–419.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. Information & Management, 54(7), 887–901.

Bennett, R. J., & Robinson, S. L. (2000). Development of a measure of workplace deviance. Journal of Applied Psychology, 85(3), 349–360. https://doi.org/10.1037/0021-9010.85.3.349

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance : The motivators and barriers of employees ' security behaviors. Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), 103–122.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151–164. https://doi.org/10.1057/ejis.2009.8

Box, D., & Pottas, D. (2014). A Model for Information Security Compliant Behaviour in the Healthcare Context. Procedia Technology, 16, 1462–1470. https://doi.org/10.1016/j.protcy.2014.10.166

Bressmann, T. (2004). Self-inflicted cosmetic tongue split: a case report. Journal (Canadian Dental Association), 70(3), 156–157. https://doi.org/10.1007/s13398-014-0173-7.2

Bryan, M. L., & Jenkins, S. P. (2016). Multilevel modelling of country effects: A cautionary tale. European Sociological Review, 32(1), 3–22.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly: Management Information Systems, 34(SPEC. ISSUE 3), 523–548. https://doi.org/10.2307/25750690

Burian, P. E., Rogerson, L., & Maffei III, F. S. (2010). The Research Roadmap: A Primer To The Approach And Process. Contemporary Issues in Education Research (CIER), 3(8), 43–58. https://doi.org/10.19030/cier.v3i8.226

Cain, M. K., Zhang, Z., & Yuan, K. H. (2017). Univariate and multivariate skewness and kurtosis for measuring nonnormality: Prevalence, influence and estimation. Behavior Research Methods, 49(5), 1716–1735. https://doi.org/10.3758/s13428-016-0814-1

Carmi, G., & Bouhnik, D. (2020). The Effect of Rational Based Beliefs and Awareness on Employee Compliance with Information Security Procedures: A Case Study of a Financial Corporation in Israel. Interdisciplinary Journal of Information, Knowledge, and Management, 15, 109–125.

Chan, H., & Mubarak, S. (2012). Significance of information security awareness in the higher education sector. International Journal of Computer Applications, 60(10).

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security at the Workplace : Linking Information Security Climate to Compliant Behavior Mark Chan National University of Singapore Irene Woon School of Computing , National University of Singapore Atreyi Kankanhalli School of Com. Journal of Information Privacy and Security, 1(3), 18–41. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.123.9572&amp;rep=rep1&amp;type=pdf

Chapple, C. L., McQuillan, J. A., & Berdahl, T. A. (2005). Gender, social bonds, and delinquency: A comparison of boys' and girls' models. Social Science Research, 34(2), 357–383.

Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. Information and Management, 55(8), 1049–1060. https://doi.org/10.1016/j.im.2018.05.011

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. Computers in Human Behavior, 38, 220–228. https://doi.org/10.1016/j.chb.2014.05.043

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 and Security, 39(PART B), 447–459. https://doi.org/10.1016/j.cose.2013.09.009

Chin. (1998). Handbook of Partial Least Squares: Concepts, Methods and Applications. Springer Berlin Heidelberg. In The Journal of biological chemistry (Vol. 206, pp. 39–49). Springer.

Chin, J. (2011). History and Context of Public Administration in Malaysia. Public Administration in East Asia, 497–516. https://doi.org/10.4324/9781315089317-27

Chin, W. W. (1998). The Partial Least Squates Approach to Structural Equation Modeling. MIS Quarterly: Management Information Systems, 22(1).

Choi, M., & Song, J. (2018). Social control through deterrence on the compliance with information security policy. Soft Computing, (2009). https://doi.org/10.1007/s00500-018-3354-z

CIA. (2019). World Threat Assessment of the US Intelligence Community. Cia, 396(2), 1119–1131. Retrieved from https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Cohen, J. (1988). Statistical power analysis for the behavioral sciences. Lawrence Erlbaum Associates. Hillsdale, NJ.

Cohen, J. (1992). A power primer. Psychological Bulletin, 112(1), 155.

Collier, J. E., & Bienstock, C. C. (2007). An analysis of how nonresponse error is assessed in academic marketing research. Marketing Theory, 7(2), 163–183. https://doi.org/10.1177/1470593107076865

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? Information Security Technical Report, 14(4), 186–196.

Connolly, L., Lang, M., & Tygar, J. D. (2015). Investigation of Employee Security Behaviour: A Grounded Theory Approach, 455(May). https://doi.org/10.1007/978-3-319-18467-8

Cybersecurity. (2021). Malaysian Public Sector Statistics.

D’Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees’ security compliance. Information Management and Computer Security, 22(5), 474–489. https://doi.org/10.1108/IMCS-08-2013-0057

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.

D’Arcy, J., & Lowry, P. B. (2017). Cognitive-affective drivers of employees’ daily compliance with information security policies: A multilevel, longitudinal study. Information Systems Journal, (October). https://doi.org/10.1111/isj.12173

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations? International Journal of Business and Society, 19(1), 161–180.

Davis, K., & Newstrom, J. W. (1977). Human Behavior At Work: Organizational Behavior, 608.

Denis, D. J. (2018). SPSS data analysis for univariate, bivariate, and multivariate statistics. John Wiley & Sons.

Depietro, R., Wiarda, E., & Fleischer, M. (1990). The context for change: Organization, technology and environment. The Processes of Technological Innovation, 199(0), 151–175.

DeVellis, R. F. (2016). Scale development: Theory and applications (Vol. 26). Sage publications.

Dhillon, G., Talib, Y. Y. A., & Picoto, W. N. (2020). The mediating role of psychological empowerment in information security compliance intentions. Journal of the Association for Information Systems, 21(1), 152–174. https://doi.org/10.17705/1jais.00595

Diachkov, D. (2018). Formation of the Information Security Policy of an Enterprise.

Draugalis, J. L. R., & Plaza, C. M. (2009). Best practices for survey research reports revisited: Implications of target population, probability sampling, and response rate. American Journal of Pharmaceutical Education, 73(8), 2–4. https://doi.org/10.5688/aj7308142

Dzazali, S., & Zolait, A. H. (2012). Assessment of information security maturity: An exploration study of Malaysian public service organizations. Journal of Systems and Information Technology.

Feng, G., Zhu, J., Wang, N., & Liang, H. (2019). How paternalistic leadership influences it security policy compliance: The mediating role of the social bond. Journal of the Association for Information Systems, 20(11), 1650–1691. https://doi.org/10.17705/1jais.00581

Fishbein, M., & Ajzen, I. (1975). Theory of Reasoned Action (TRA).

Fishbein, M., & Ajzen, I. (2011). Predicting and changing behavior: The reasoned action approach. Psychology press.

Fornell, C., & Larcker, D. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research.

Friesen, L. (2012). Certainty of punishment versus severity of punishment: An experimental investigation. Southern Economic Journal, 79(2), 399–421.

Furnell, S. (2006). Malicious or misinformed? Exploring a contributor to the insider threat. Computer Fraud & Security, 9(2006), 8–12.

Gangire, Y., Da Veiga, A., & Herselman, M. (2019). A conceptual model of information security compliant behaviour based on the self-determination theory. 2019 Conference on Information Communications Technology and Society, ICTAS 2019. https://doi.org/10.1109/ICTAS.2019.8703629

Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's comments: an update and extension to SEM guidelines for administrative and social science research. Mis Quarterly, iii–xiv.

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice. Communications of the Association for Information Systems, 4(August). https://doi.org/10.17705/1cais.00407

Geisser, S. (1974). A predictive approach to the random effect model. Biometrika, 61(1), 101–107. https://doi.org/10.1093/biomet/61.1.101

Gibbs, J. P. (1975). Crime, punishment, and deterrence. Elsevier New York.

Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: An organizational capabilities perspective. Journal of Management Information Systems, 18(1), 185–214. https://doi.org/10.1080/07421222.2001.11045669

Goodboy, A. K., & Kline, R. B. (2017). Statistical and Practical Concerns With Published Communication Research Featuring Structural Equation Modeling. Communication Research Reports, 34(1), 68–77. https://doi.org/10.1080/08824096.2016.1214121

Gough, D., Oliver, S., & Thomas, J. (2017). An introduction to systematic reviews. Sage.

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.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2018). Partial least squares structural equation modeling (PLS-SEM). Sage Publisher. Retrieved from http://www.emeraldinsight.com/doi/abs/10.1108/EBR-10-2013-0128%5Cnhttp://www.emeraldinsight.com/10.1108/EBR-10-2013-0128

Hair, J., Hollingsworth, C. L., Randolph, A. B., & Chong, A. Y. L. (2017). An updated and expanded assessment of PLS-SEM in information systems research. Industrial Management and Data Systems, 117(3), 442–458. https://doi.org/10.1108/IMDS-04-2016-0130

Hair, Joe F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. Journal of Marketing Theory and Practice, 19(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hair, Joe F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. European Business Review, 26(2), 106–121. https://doi.org/10.1108/EBR-10-2013-0128

Hair, Joseph F. (2007). Research Methods for Business. Education + Training (Vol. 49). John Wiley & Sons. https://doi.org/10.1108/et.2007.49.4.336.2

Hair, Joseph F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., & Thiele, K. O. (2017). Mirror, mirror on the wall: a comparative evaluation of composite-based structural equation modeling methods. Journal of the Academy of Marketing Science, 45(5), 616–632. https://doi.org/10.1007/s11747-017-0517-x

Hair, Joseph F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. European Business Review, 31(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

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. https://doi.org/10.1016/j.cose.2016.12.016

Hayes, A. F., & Scharkow, M. (2013). The Relative Trustworthiness of Inferential Tests of the Indirect Effect in Statistical Mediation Analysis: Does Method

Really Matter? Psychological Science, 24(10), 1918–1927. https://doi.org/10.1177/0956797613480187

Haynes, S. N., Richard, D. C. S., & Kubany, E. S. (1995). Content Validity in Psychological Assessment: A Functional Approach to Concepts and Methods. Psychological Assessment, 7(3), 238–247. https://doi.org/10.1037/1040-3590.7.3.238

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. https://doi.org/10.1007/s11747-014-0403-8

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hina, S., & Dominic, D. D. (2017). Compliance : A Perspective in Higher Education Institutions. Proceedings of the 5th International Conference on Research and Innovation in Information Systems, 1–6.

Hirschi, T. (1969). A control theory of delinquency. Criminology Theory: Selected Classic Readings, 1969, 289–305.

Hofeditz, M., Nienaber, A. M., Dysvik, A., & Schewe, G. (2017). “Want to” Versus “Have to”: Intrinsic and Extrinsic Motivators as Predictors of Compliance Behavior Intention. Human Resource Management, 56(1), 25–49. https://doi.org/10.1002/hrm.21774

Howard, P. D. (2003). Security Policy Lifecycle: Functions and Responsibilities. In H. F. Tipton & M. Krause (Eds.), Information Security Management (1st Editio). Auerbach Publications.

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.

Humaidi, N., Balakrishnan, V., & Shahrom, M. (2014). Exploring user’s compliance behavior towards Health Information System security policies based on extended Health Belief Model. 2014 IEEE Conference on E-Learning, e-Management and e-Services (IC3e), 30–35. https://doi.org/10.1109/IC3e.2014.7081237

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, 45(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information and Management, 51(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Ifinedo, P. (2018). Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions. Information Resources Management Journal, 31(1), 53–82. https://doi.org/10.4018/IRMJ.2018010103

Iriqat, Y. M., Ahlan, A. R., & Molok, N. N. A. (2019). Information security policy perceived compliance among staff in palestine universities: An empirical pilot study. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, JEEIT 2019 - Proceedings, 580–585. https://doi.org/10.1109/JEEIT.2019.8717438

ISO/IEC. (2013). ISO/IEC 27002. Iec. Retrieved from www.iso.org

ISO/TS 21547. (2010). ISO/TS 21547.

Johnson, R. E., Rosen, C. C., & Chang, C. H. (2011). To Aggregate or Not to Aggregate: Steps for Developing and Validating Higher-Order Multidimensional Constructs. Journal of Business and Psychology, 26(3), 241–248. https://doi.org/10.1007/s10869-011-9238-1

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. MIS Quarterly, 39(1), 113–134. https://doi.org/10.25300/MISQ/2015/39.1.06

Joyce, W. F., & Slocum, J. W. (1984). Collective Climate: Agreement as a Basis for Defining Aggregate Climates in Organizations . Academy of Management Journal, 27(4), 721–742. https://doi.org/10.5465/255875

Kim, S. H., Yang, K. H., & Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. The Scientific World Journal, 2014, 1–12. https://doi.org/10.1155/2014/463870

Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering Executive summary.

Kline, R. B. (2011). Convergence of structural equation modeling and multilevel modeling. na.

Kock, N. (2017). Which is the Best Way to Measure Job Performance. International Journal of E-Collaboration, 13(2), 1–9. https://doi.org/10.4018/ijec.2017040101

Koole, S. L., Schlinkert, C., Maldei, T., & Baumann, N. (2018). Becoming Who You Are: An Integrative Review of Self-Determination Theory and Personality Systems Interactions Theory. Journal of Personality, (February). https://doi.org/10.1111/jopy.12380

Kranz, J., & Haeussinger, F. (2014). Why deterrence is not enough : The role of endogenous motivations on employees? information security behavior, (December).

Kristjansson, E. A., Desrochers, A., & Zumbo, B. (2003). Translating and adapting measurement instruments for cross-linguistic and cross-cultural research: A guide for practitioners. Canadian Journal of Nursing Research, 35(2), 127–142.

Lamers, S. M. A., Westerhof, G. J., Bohlmeijer, E. T., Ten Klooster, P. M., & Keyes, C. L. M. (2011). Evaluating the psychometric properties of the mental health Continuum-Short Form (MHC-SF). Journal of Clinical Psychology, 67(1), 99–110. https://doi.org/10.1002/jclp.20741

Larose, R., & Rifon, N. (2006). Your privacy is assured of being disturbed: Websites with and without privacy seals. New Media and Society, 8(6), 1009–1029. https://doi.org/10.1177/1461444806069652

Lawshe, C. H. (1975). a Quantitative Approach To Content Validity. Personnel Psychology, 28(4), 563–575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. Management Research Review, 37(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. Information Management & Computer Security, 10(2), 57–63. https://doi.org/10.1108/09685220210424104

Legault, L. (2020). Encyclopedia of Personality and Individual Differences. Encyclopedia of Personality and Individual Differences, (October). https://doi.org/10.1007/978-3-319-28099-8

Lindner, J. R., Murphy, T. H., & Briers, G. E. (2001). Handling nonresponse in social science research. Journal of Agricultural Education, 42(4), 43–53.

Liu, Chenhui, Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. International Journal of Information Management, 54(28), 102152. https://doi.org/10.1016/j.ijinfomgt.2020.102152

Liu, Chongrui, Wang, C., Wang, H., & Niu, B. (2020). Influencing factors of employees’ information systems security policy compliance: An empirical research in China. In E3S Web of Conferences (Vol. 218). EDP Sciences.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Information Systems Journal, 25(5), 433–463. https://doi.org/10.1111/isj.12043

Luarn, P., & Lin, H. H. (2005). Toward an understanding of the behavioral intention to use mobile banking. Computers in Human Behavior, 21(6), 873–891. https://doi.org/10.1016/j.chb.2004.03.003

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. Management Science, 52(12), 1865–1883. https://doi.org/10.1287/mnsc.1060.0597

MAMPU. (2001). Malaysian Public Sector Management Of Information & Communications Technology Security Handbook (MyMIS).

MAMPU. (2010). Dasar Keselamatan ICT. Retrieved from http://www.mampu.gov.my/ms/warga-mampu/dasar-keselamatan-ict

MAMPU. (2016). Rangka kerja keselamatan Siber Sektor Awam (RAKKSSA).

MAMPU. (2021). Pendigitalan Sektor Awam 2021-2025.

Matthews, L., Hair, J., & Matthews, R. (2018). PLS-SEM: The Holy Grail for Advanced Analysis. The Marketing Management Journal, 28(1), 1–13. Retrieved from http://www.mmaglobal.org/publications/MMJ/MMJ-Issues/2018-Spring/MMJ-2018-Vol28-Issue1-Complete.pdf#page=9

McClelland, D. C., & Boyatzis, R. E. (1982). Leadership motive pattern and long-term success in management. Journal of Applied Psychology, 67(6), 737.

Mellahi, K., & Harris, L. C. (2016). Response Rates in Business and Management Research: An Overview of Current Practice and Suggestions for Future Direction. British Journal of Management, 27(2), 426–437. https://doi.org/10.1111/1467-8551.12154

Memon, M. A., 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(June), i–xiii. https://doi.org/10.47263/jasem.1(1)01

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. Journal of Management Information Systems, 34(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioral Sciences, 147(August), 424–428. https://doi.org/10.1016/j.sbspro.2014.07.133

Miron, A. M., & Brehm, J. W. (2006). Reactance Theory - 40 Years Later. Zeitschrift Fur Sozialpsychologie, 37(1), 9–18. https://doi.org/10.1024/0044-3514.37.1.9

Moody, G. D., Siponen, M., & Pahnila, S. Toward a unified model of information security policy compliance, 42 MIS Quarterly: Management Information Systems § (2018). https://doi.org/10.25300/MISQ/2018/13853

Mubarak, S. (2016). Developing a theory-based information security management framework for human service organizations. Journal of Information, Communication and Ethics in Society, 14(3), 254–271. https://doi.org/10.1108/JICES-06-2015-0018

Muhire, B. (2012). Employee Compliance with Information Systems Security Policy in Retail Industry. Case: Store Level Employees. Honors Thesis Program in the College of Management. Retrieved from http://scholarworks.umb.edu/management_hontheses/12

MyCERT. (2014). MyCERT Incident Statistics for the year 2014. Retrieved from http://www.mycert.org.my/en/services/statistic/mycert/2014/main/detail/949/index.html

MYCERT. (2020). MyCERT Incident Statistics 2020.

Nasir, A., Rashid, M., & Hamid, A. (2017). Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture : A Conceptual Framework, 56–60.

Nastase, H. (2007). Introduction to AdS-CFT. Proceedings of the 12th Annual International Digital Government Research Conference on Digital Government Innovation in Challenging Times - dg.o ’11. https://doi.org/10.18235/0000407

National Security Council. (2019). Malaysia CyberSecurity Strategy 2020-2024. Retrieved from https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf

Ng, B. Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying users’ computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Nor’ashikin, A., Tretiakov, A., & Whiddett, D. (2014). A content validity study for a knowledge management systems success model in healthcare. Journal of Information Technology Theory and Application, 15(2), 21–36.

Okoli, C. (2015). A guide to conducting a standalone systematic literature review. Communications of the Association for Information Systems, 37(1), 43.

Okoli, C., & Schabram, K. (2012). A Guide to Conducting a Systematic Literature Review of Information Systems Research. SSRN Electronic Journal, 10(2010), 51. https://doi.org/10.2139/ssrn.1954824

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures. ACM Transactions on Management Information Systems, 12(2), 1–29. https://doi.org/10.1145/3424282

Oreg, S. (2012). Resistance to change scale. Cases and Exercises in Organization Development and Change, 88(4), 302–305. https://doi.org/10.4135/9781483387444.n37

Organ, D. W., Podsakoff, P. M., & MacKenzie, S. B. (2006). Organizational citizenship behavior: Its nature, antecedents, and consequences. Organizational

Citizenship Behavior: Its Nature, Antecedents, and Consequences. Sage Publications. https://doi.org/10.4135/9781452231082

Ouchi, W. G., & Maguire, M. A. (1975). Organizational control: Two functions. Administrative Science Quarterly, 559–569.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. Computers and Security, 31(5), 673–680. https://doi.org/10.1016/j.cose.2012.04.004

Pagano, R. R. (2012). Understanding statistics in the behavioral sciences. Cengage Learning.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. Pacis, 2007. Retrieved from http://aisel.aisnet.org/pacis2007/73

Pallant, J. (2016). EBOOK: SPSS Survival Manual. McGraw-Hill Education (UK).

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: a comparison of two studies. Information & Computer Security.

Petticrew, M., & Roberts, H. (2008). Systematic reviews in the social sciences: A practical guide. John Wiley & Sons.

Pham, H. C., El-Den, J., & Richardson, J. (2016). Stress-based security compliance model - An exploratory study. Information and Computer Security, 24(4), 326–347. 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. Journal of Applied Psychology, 88(5), 879–903. https://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. Annual Review of Psychology, 63, 539–569. https://doi.org/10.1146/annurev-psych-120710-100452

Podsakoff, P. M., & Organ, D. W. (1986). Podsakoff & Organ 1986.pdf. Journal of Management.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. Journal of Management Information Systems, 32(4), 179–214.

Quinn, R. E., & Rohrbaugh, J. (1983). A spatial model of effectiveness criteria: Towards a competing values approach to organizational analysis. Management Science, 29(3), 363–377.

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. Computers and Security, 80, 211–223. https://doi.org/10.1016/j.cose.2018.09.016

Ramayah, T., Yeap, J. A. L., & Ignatius, J. (2013). An Empirical Inquiry on Knowledge Sharing Among Academicians in Higher Learning Institutions. Minerva, 51(2), 131–154. https://doi.org/10.1007/s11024-013-9229-7

Ramayah, T., Yeap, J. A. L. J., Ahmad, N. N. H., Abdul-Halim, H., Rahman, S. A., & Halim, H. (2017). Testing a Confirmatory model of Facebook Usage in SmartPLS using Consistent PLS. International Journal of Business and Innovation, 3(2), 1–14.

Razilan, M., Kadir, A., Norwahidah, S., Norman, S., Rahman, S. A., & Bunawan, A. (2016). Information Security Policies Compliance among Employees in Cybersecurity Malaysia. In Proceedings of the 28th International Business Information Management Association Conference.

Ringle, C. M., & Sarstedt, M. (2016). Gain more insight from your PLS-SEM results the importance-performance map analysis. Industrial Management and Data Systems, 116(9), 1865–1886. https://doi.org/10.1108/IMDS-10-2015-0449

Rip, A., & Modulation, T. (2008). Processes of Technological Innovation in Context. October. Lexington books.

Rodgers, R. F., Rich, J. M., & DeVitis, J. L. (1986). Theories of Moral Development. The Journal of Higher Education (Vol. 57). Charles C Thomas, Publisher. https://doi.org/10.2307/1981260

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. The Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rönkkö, M., & Ylitalo, J. (2011). PLS marker variable approach to diagnosing and controlling for method variance.

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. American Psychologist, 55(1), 68–78. https://doi.org/10.1037/0003-066X.55.1.68

Safa, N. S., Solms, R. Von, & Futcher, L. (2016). Human aspects of information security in organisations. Computer Fraud and Security, 2016(2), 15–18. https://doi.org/10.1016/S1361-3723(16)30017-3

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers and Security, 53, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Salleh, N., Mendes, E., & Grundy, J. C. (2011). Empirical studies of pair programming for CS/SE teaching in higher education: A systematic literature review. IEEE Transactions on Software Engineering, 37(4), 509–525. https://doi.org/10.1109/TSE.2010.59

Sandberg, T., & Conner, M. (2008). Anticipated regret as an additional predictor in the theory of planned behaviour: A meta-analysis. British Journal of Social Psychology, 47(4), 589–606. https://doi.org/10.1348/014466607X258704

Santos, J. R. A. (1999). Cronbach’s alpha: A tool for assessing the reliability of scales. Journal of Extension, 37(2), 1–5.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students. Pearson education.

Schwartz, S. H. (1977). Normative Influences on Altruism ’, (September).

Scott Armstrong, J., & Overton Marketing Scientist, T. S. (1977). Estimating Nonresponse Bias in Mail Surveys. Journal of Marketing Research, 14, 396–402.

Shamsudin, N. N. A., Yatin, S. F. M., Nazim, N. F. M., Talib, A. W., Sopiee, M. A. M., & Shaari, F. N. (2019). Information Security Behaviors among Employees. International Journal of Academic Research in Business and Social Sciences, 9(6), 337–349. https://doi.org/10.6007/IJARBSS/v9-i6/5972

Shaw, D., Gorely, T., & Corban, R. (2020). C2. Cognitive evaluation theory. BIOS Instant Notes in Sport and Exercise Psychology. https://doi.org/10.4324/9780203325568-23

Shmueli, G., Ray, S., Velasquez Estrada, J. M., & Chatla, S. B. (2016). The elephant in the room: Predictive performance of PLS models. Journal of Business Research, 69(10), 4552–4564. https://doi.org/10.1016/j.jbusres.2016.03.049

Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J. H., Ting, H., Vaithilingam, S., & Ringle, C. M. (2019). Predictive model assessment in PLS-SEM: guidelines for using PLSpredict. European Journal of Marketing, 53(11), 2322–2347. https://doi.org/10.1108/EJM-02-2019-0189

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management." Journal of Enterprise Information Management, 27(5), 644–667. https://doi.org/10.1108/JEIM-07-2013-0052

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information and Management, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. European Journal of Information Systems, 23(3), 289–305. https://doi.org/10.1057/ejis.2012.59

Soffian;, S. I. S., Ismail;, E. A. E., Hanim, H. F. F., & Hassan, H. (2011). Public Sector Accounting and Financial Management in Malaysia. Pearson Custom Publishing. Retrieved from https://books.google.com.my/books?id=isa3ngEACAAJ

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers and Security, 56, 1–13. https://doi.org/10.1016/j.cose.2015.10.006

Sommestad, T. (2018). Work-related groups and information security policy compliance. Information and Computer Security, 26(5), 533–550. https://doi.org/10.1108/ICS-08-2017-0054

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management and Computer Security, 22(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information and Computer Security, 23(2), 200–217. https://doi.org/10.1108/ICS-04-2014-0025

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stewart, H., & Jurjens, J. (2017). Information security management and the human aspect in organizations. Information and Computer Security, 25(5), 494–534. https://doi.org/10.1108/ICS-07-2016-0054

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. Journal of the Royal Statistical Society: Series B (Methodological), 36(2), 111–133.

Straub, D., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. Communications of the Association for Information Systems, 13(1), 24. https://doi.org/10.17705/1cais.01324

Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. American Sociological Review, 22(6), 664. https://doi.org/10.2307/2089195

Tabachnick, B. G., & Fidell, L. S. (2014). Using multivariate statistics new international edition. Pearson2012, 1055.

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. https://doi.org/10.20547/jms.2014.1704202

Teoh, C. S., Mahmood, A. K., & Dzazali, S. (2018). Cyber Security Challenges in Organisations: A Case Study in Malaysia. In 2018 4th International Conference on Computer and Information Sciences (ICCOINS) (pp. 1–6).

Torrance, E. P., & Brehm, J. W. (1968). A Theory of Psychological Reactance. The American Journal of Psychology, 81(1), 133. https://doi.org/10.2307/1420824

Trang, S., & Brendel, B. (2019). A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. Information Systems Frontiers. https://doi.org/10.1007/s10796-019-09956-4

Triandis, H. C. (1977). Interpersonal behavior. Brooks/Cole Pub. Co.

Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. Computers and Security, 59(1318885), 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Tu, C. Z., Adkins, J., Zhao, G. Y., & Adkins, J. (2019). A Review of Information Systems Security Management : An Integrated Framework.

Tuffield, D. (1975). Organisation behaviour. Industrial and Commercial Training, 7(4), 164–166. https://doi.org/10.1108/eb003462

Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. Academy of Management Journal, 48(6), 1143–1158.

Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. Journal of Information Technology Theory and Application, 11(2), 5–40.

Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. Journal of the Association for Information Systems, 17(7), 435–495. https://doi.org/10.17705/1jais.00433

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly: Management Information Systems, 27(3), 425–478. https://doi.org/10.2307/30036540

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy. Journal of Information Privacy and Security, 9(4), 52–79. https://doi.org/10.1080/15536548.2013.10845690

Wang, S., & Noe, R. A. (2010). Knowledge sharing: A review and directions for future research. Human Resource Management Review, 20(2), 115–131. https://doi.org/10.1016/j.hrmr.2009.10.001

Wang, X., & Xu, J. (2021). Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry. Tourism Management, 84, 104282. https://doi.org/10.1016/j.tourman.2021.104282

Williams, L. J., Hartman, N., & Cavazotte, F. (2010). Method variance and marker variables: A review and comprehensive cfa marker technique. Organizational Research Methods, 13(3), 477–514. https://doi.org/10.1177/1094428110366036

Wilson, S. R., & Vucetic, J. (2016). Information security awareness in higher education: A qualitative case study investigation. ProQuest Dissertations and Theses.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. Communication Monographs, 59(4), 329–349. https://doi.org/10.1080/03637759209376276

Yazdanmehr, A., & Wang, J. (2016). Employees’ information security policy compliance: A norm activation perspective. Decision Support Systems, 92, 36–46. https://doi.org/10.1016/j.dss.2016.09.009

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. Information Technology and People, 26(4), 401–419. https://doi.org/10.1108/ITP-12-2012-0147

LIST OF PUBLICATIONS

Indexed Journal

1. **Kuppusamy, P.,** Samy, G. N., Maarop, N., Shanmugam, B., & Perumal, S. (2022). Information Security Policy Compliance Behavior Models, Theories, And Influencing Factors: A Systematic Literature Review. *Journal Of Theoretical And Applied Information Technology*, *100*(5) (**Indexed by SCOPUS**)

Indexed Conference Proceedings

1. **Kuppusamy, P**., Samy, G. N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B., & Perumal, S. (2020, May). Systematic literature review of information security compliance behaviour theories. In *Journal of physics: conference series* (Vol. 1551, No. 1, p. 012005). IOP Publishing (**Indexed by SCOPUS**)