NATIONAL INFORMATION INFRASTRUCTURE ORGANISATIONS AND CYBER SECURITY COMPLIANCE IN MALAYSIA

MASLINA BINTI DAUD

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

FACULTY OF ECONOMICS AND ADMINISTRATION
UNIVERSITY OF MALAYA
KUALA LUMPUR

2018

UNIVERSITY OF MALAYA
ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: MASLINA BINTI DAUD [redacted]

Matric No: EHA120001

Name of Degree: DOCTOR OF PHILOSOPHY

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

NATIONAL INFORMATION INFRASTRUCTURE ORGANISATIONS AND CYBER SECURITY COMPLIANCE IN MALAYSIA

Field of Study: INFORMATION SECURITY AND ECONOMICS

I do solemnly and sincerely declare that:

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

(2) This Work is original;

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

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

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

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

Candidate's Signature [redacted] Date: 4-7-18

Subscribed and solemnly declared before,

Witness's Signature [redacted] Date: 4-7-18

Name: RAJAH RASIAH

Designation: DISTINGUISHED PROFESSOR

NATIONAL INFORMATION INFRASTRUCTURE ORGANISATIONS AND CYBER SECURITY COMPLIANCE IN MALAYSIA

ABSTRACT

The constant increase in cyber security breaches (CSB) has raised concerns globally mainly due to deviant behaviour of employees. Previous studies have claimed that a lack of security technologies and capabilities have contributed to these breaches. Despite increasing cyber security investment, organisations continue to experience security breaches. In light of the non-excludability of cyber security as a public good, this study seeks to examine factors that stimulate cooperation to comply with security requirements to prevent security breaches. However, little work has examined the relationship between non-excludability of cyber security and cooperative behaviour to achieve cyber security compliance (CSC) in organisations. Hence, this thesis presents an in-depth analysis of cooperation to address CSC in critical national information infrastructure (CNII) sectors in Malaysia. Specifically, this study aims to: i) investigate factors that influence employees' cooperative behavioural intentions (ITC) in achieving CSC; ii) analyse the mediation effect of organisational security practices by employees' cooperative behaviour in promoting CSC; and iii) identify the effectiveness of cyber security governance instruments implemented at organisational, sectoral and national levels in Malaysia. A representative sample of 155 organisations with 69.7 % from a population of 220 from these sectors participated in this study. The important CSC factors were included: effective security awareness (ESA), technical capability (TC), security role (SR) and institutional role (IR) (which constitute cooperation), top management commitment (TMC), structured security processes (SSP), security investment (SI) and organizational, sectoral and national governance instruments sectoral and national governance instruments. Various statistical methods including binary logistic regression, Karlson Holm and Breen method and ordinal logistic regression were deployed to answer each research question. The findings were subsequently confirmed by face-to-face interviews. The findings show that ESA (OR = 2.561, p = 0.04), SR for top management (OR = 3.224, p = 0.06) and middle management (OR = 2.759, p = 0.020) and IR (OR = 1.528, p = 0.044) significantly predict ITC. Employees’ ITC can be strengthened by instilling a sense of belongingness through ESA and internalisation of IR to behave altruistically to achieve a common goal. The findings also show that large workforce organisations (OR = 0.342, p = 0.026) are less likely to contribute to ITC, indicating that opportunistic behaviour looms strongly in large groups. Furthermore, ITC contributed significantly (OR = 0.067, p = 0.001) to employees’ cooperation in organizations. The results also show that cooperation partially mediates the relationship between both TMC (OR = 0.222, p = 0.002) and SSP (OR = 1.555, p = 0.006) with CSC, where SSP has stronger mediation effect (30.63 %) than TMC (16.67 %). This study also shows how inter-related tasks embedded in security processes require cooperative and collective efforts to promote CSC, in which security information and knowledge are transferred in a structured and systematic manner. Finally, this thesis shows that cyber security governance instruments implemented in organisations (OR = 2.469, p = 0.000) and at national level (OR = 4.242, p = 0.003) are more likely to be more effective than across sectors in achieving CSC in organisations.

Keywords: cooperation, cyber security compliance, organisational security practices, security governance, institutions

ORGANISASI INFRASTRUKTUR MAKLUMAT NEGARA DAN PEMATUHAN KESELAMATAN SIBER DI MALAYSIA

ABSTRAK

Peningkatan yang konsisten dalam pelanggaran keselamatan siber (CSB) telah menimbulkan kebimbangan secara global terutamanya disebabkan oleh penyimpangan tingkah laku pekerja. Kajian terdahulu menunjukkan bahawa kekurangan keupayaan dan keselamatan teknologi menyumbang kepada pelanggaran ini. Walaupun terdapat peningkatan dalam pelaburan keselamatan siber, namun organisasi berterusan mengalami pelanggaran keselamatan siber. Berdasarkan tiada sifat pengecualian keatas keselamatan siber sebagai suatu barangan awam, kajian ini berusaha untuk mengkaji faktor-faktor yang merangsang kerjasama dalam mematuhi keperluan keselamatan bagi mencegah pelanggaran tersebut. Namun, hanya sedikit usaha dilakukan dalam mengkaji hubungan di antara pengecualian tersebut dan tingkah laku kerjasama untuk mencapai pematuhan keselamatan siber (CSC) dalam organisasi. Oleh itu, tesis ini membentangkan analisis kerjasama yang mendalam untuk menangani CSC dalam sektor-sektor infrastruktur maklumat kritikal negara (CNII) di Malaysia. Secara khusus, kajian ini bertujuan untuk: i) menyelidik faktor-faktor yang mempengaruhi niat tingkah laku bekerjasama pekerja dalam mencapai CSC; ii) mendalami kesan pengantaraan amalan keselamatan organisasi melalui kerjasama tingkah laku pekerja (ITC) dalam menggalakkan CSC; dan iii) mengenalpasti keberkesanan instrumen tadbir keselamatan keselamatan siber yang dilaksanakan di peringkat organisasi, sektor dan kebangsaan di Malaysia. Sample sebanyak 155 organisasi iaitu 69.7 peratus daripada 220 organisasi dalam sektor-sektor tersebut telah mengambil bahagian. Faktor-faktor penting CSC termasuklah: kesedaran keselamatan yang efektif (ESA), keupayaan teknikal (TC), peranan keselamatan (SR) dan institusi (IR), komitmen pengurusan atasan (TMC), proses keselamatan berstruktur (SSP), pelaburan keselamatan (SI), kepimpinan keselamatan (SL), struktur urus tadbir keselamatan (SGS), audit keselamatan maklumat (ISA), dan instrumen sektor tadbir urus bagi sektoral dan nasional. Pelbagai kaedah statistik termasuk regresi logistik binari, kaedah Karlson Holm dan Breen dan regresi logistik ordinal telah digunakan dalam kajian ini. Penemuan kajian ini disokong oleh temuduga dengan responden. Penemuan kajian menunjukkan bahawa ESA (OR = 2.561, p = 0.04), SR untuk pengurusan atasan (OR = 3.224, p = 0.06) dan pertengahan (OR = 2.759, p = 0.020) dan IR (OR = 1.528, p = 0.044) menjangkakan ITC secara signifikan. ITC dalam kalangan pekerja dapat dikukuhkan dengan menanam rasa kepunyaan melalui ESA dan pengaruh dalaman melalui IR untuk mereka bertindak secara altruistik bagi mencapai matlamat yang sama. Penemuan ini juga menunjukkan bahawa organisasi yang mempunya tenaga kerja yang besar (OR = 0.342, p = 0.026) kurang menyumbang kepada ITC, dimana tingkah oportunistik pekerja tercetus apabila mereka berada di dalam kumpulan yang besar. ITC menyumbang secara signifikan (OR = 0.067, p = 0.001) keatas kerjasama pekerja didalam organisasi. Hasil kajian juga menunjukkan bahawa kerjasama boleh menjadi pengantara di antara TMC (OR = 0.222, p = 0.002) dan SSP (OR = 1.555, p = 0.006) dengan CSC, dimana SSP menghasilkan kesan pengantaraan yang lebih kuat (30.63 peratus) berbanding dengan TMC (16.67 peratus). Kajian ini juga menunjukkan keterkaitan tugas memerlukan kerjasama dan usaha secara kolektif bagi mempromosikan CSC, di mana maklumat dan pengetahuan keselamatan dapat dipindahkan secara tersusun dan sistematik. Tesis ini menunjukkan bahawa instrumen tadbir urus keselamatan siber yang dilaksanakan diperingkat organisasi (OR = 2.469, p = 0.000) dan diperingkat kebangsaan (OR = 4.242, p = 0.003) adalah lebih berkesan daripada di peringkat sektor dalam mencapai CSC di dalam organisasi.

Kata kunci: kerjasama, pematuhan keselamatan siber, amalan-amalan keselematan organisasi, tadbir urus keselamatan, institusi

ACKNOWLEDGEMENTS

I would like to express my gratitude to my main supervisor, Distinguished Professor Dr. Rajah Rasiah who gave me a complete guidance and encouragement and showed me the way throughout the whole process. Also to Datin Professor Dr. Mary George who frequently sat together assisting me and supporting me in every way she could. Not to forget Assoc. Prof. Dr. David Asirvatham who helped me at the very early stage of my journey. I would also like to thank Ms. Govindamal Thangiah who helped me in performing a better statistical analysis for me to keep on moving. I would like to dedicate this thesis to my mother Badariah, my son Amiroul and my daughter, Amanda for their support over the years. No doubts it has been a journey with challenges and stress; juggling my time with my busy work schedule and family matters. But, they had been patient and tolerable enough throughout this journey. I would like also to dedicate this thesis to my late father who was very supportive upon knowing that I wanted to pursue my study though at a later age. Although he had gone even before I even started, the completion of this thesis fulfils his wishes to have at least one of his children to have this level of achievement that would have made him proud. I would also like to thank my friends and colleagues who gave me all the support that I needed. Lastly, I would also like to thank CyberSecurity Malaysia for the support given to me in finishing up this thesis.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATION

BCM	:	Business Continuity Management
BLR	:	Binary Logistic Regression
CB	:	Cooperative Behaviour
CCA	:	Computer Crimes Act 1997
CERT	:	Computer Emergency Response Team
CIO	:	Chief Information Officer
CISO	:	Chief Information Security Officer
CMA	:	Communications and Multimedia Act 1998
COBIT	:	Control Objectives for Information and Related Technologies
CSIRT	:	Computer Security Incident Response Team
CSL	:	Cyber Security Leadership
DDoS	:	Distributed Denial of Service
DV	:	Dependent Variable
FISMA	:	Federal Information Security Management Act
GCERT	:	Government Computer Emergency Response Team
GSOC	:	Government Security Operations Centre
HIPPA	:	Health Insurance Portability and Accountability Act
ICT	:	Information and Communications Technology
IDS	:	Intrusion Detection System
IMP	:	Incident Management Procedure
IoT	:	Internet of Thing
IP	:	Intellectual Property
IPS	:	Intrusion Prevention System
IS	:	Information Security
ISA	:	Information Security Audit

ISAC	:	Information Sharing & Analysis Centres
ISM	:	Information Security Manager
ISMS	:	Information Security Management System
ISO	:	International Standard Organisation
ISP	:	Internet Service Provider
IT	:	Information Technology
ITC	:	Intention to Cooperate
IV	:	Independent Variables
KHB	:	Karlson-Holm-Breen
MAMPU	:	Malaysian Administrative Modernisation and Management Planning Unit
MCDISMS	:	Malaysian Cabinet Directive for ISMS Implementation
MOSTI	:	Ministry of Science Technology and Innovation
NCCMRCCP	:	National Cyber Crisis Management Response, Communication and Coordination Procedure
NCSG	:	National Cyber Security Governance
NCSP	:	National Cyber Security Policy
NC4	:	National Cyber Coordination and Command Centre
NSC	:	National Security Council
NSC24	:	National Security Directive No 24
OCSG	:	Organisational Cyber security Governance
OLR	:	Ordinal Logistic Regression
OR	:	Odds Ratio
PCI-DSS	:	Payment Card Industry Data Security Standard
PII	:	Personal Identifiable Information
SCADA	:	Supervisory Control and Data Acquisition
SCSG	:	Sectoral Cyber Security Governance

SD	:	Standard Deviation
SI	:	Security Investment
SME	:	Small Medium Enterprises
SOX	:	Sarbanes-Oxley Act
SSP	:	Structured Security Processes
TMC	:	Top Management Commitment
TPB	:	Theory of Planned Behaviour
US	:	United States
VIF	:	Variation Inflation Factor

LIST OF APPENDICES

CHAPTER 1: INTRODUCTION

1.1 Introduction

The exponential growth in new technologies is not only raising interconnectivities but also has made the Internet a part of daily life. The way businesses are carried out today demands increasing interconnectivities and interdependencies that requires the use of the Internet (Ifinedo, 2014; World Economic Forum, 2015). On the dark side of it, this situation introduces new threats. Unfortunately, the adoption of fast growing technologies, such as smart phones and cloud computing services in organisations is not aligned to the security knowledge captured by Internet users. This gap has created opportunities by certain quarters for adverse motives. The impact of laxity of businesses, image and reputation due to cyber security breaches are not only the responsibility of executive managements, but also of corporate board members. In recent years, major security breaches have made headlines signalling organisations that cyber security breaches (Deac, 2015; Robertson & Riley, 2014) can occur anytime if organisations are not prepared. For example, security breaches experienced by Yahoo was dubbed as the biggest security breaches ever[1] (Armerding, 2018) and Target's breaches resulted in the resignation of its CEO and board members[2] (Armerding, 2018; Basu, 2014). Although top-down approaches have been considered more successful in managing security in organisations, these lapses have led to many calling for emphasis to be placed on employees. Thus, security is increasingly becoming everyone's responsibility (Wylder, 2003). In Target's case, late response in acting over early warnings about cyber security

[1] Cyber attack on Yahoo was possibly conducted by "a state sponsored actor" in year 2014 compromised Personal Identifiable Information (PII) such as real names, email addresses, date of birth and telephone numbers of 500 million users. However, in October 2017, Yahoo confirmed the actual affected user accounts were 3 billions.

[2] Security breaches on Target occurred before Thanksgiving in year 2013 but only discovered several weeks after the incident. Hackers gained access to the point of sale system payment card readers through a third-party air-conditioning system vendor. By January 2014, the company estimated that 70 million of its customers' details were stolen.

breaches caused by human error by its security team left Target with massive cyber security related costs globally (Riley et al., 2014).

Security scholars have been studying the impact of cyber security breaches from the aspect of people (Bresz, 2004; Sasse, Brostoff, & Weirich, 2001; Vroom & Von Solms, 2004), processes (Gonzalez, 2005) and technology (Ben-Asher & Gonzalez, 2015; Von Solms, 1997). Yet, there have been limited studies to identify how people function in the chain of cyber security, and the determinants of security efforts targeted at protection.

As cyber security breaches have increased since 2000, efforts to model problems of information security have largely emerged from microeconomic research. The three major theories that have grappled with the issue include information as a public good, and hence, its associated theories related to externalities, free-riders, and asymmetric information (Baumol & Oates, 1988; Stigler, 1974; Stiglitz, 1985). As users in cyber space have grown rapidly, it is important to understand human behaviour to formulate policies that can check its abuse.

Information security problems is related more to the discipline of economics rather than technology (Anderson, 2001; Anderson & Moore, 2006; Schneier, 2007; Zahri Yunos et al., 2010). Referring to software vulnerabilities as a security issue where the cost of the state of insecurity due to these vulnerabilities have largely been passed down to users (either individuals or organisations), Schneier (2007) suggested that the associated externality issues had to be fixed in order to improve information security. Thus, having an understanding of the underlying economic factors is as important as the technical design to achieve reliable, trustworthy and secure Information Communications Technology (ICT) environment. Security researchers (Adar & Huberman, 2000; Greco & Floridi, 2004; Lukasik, 2011; Rosenzweig, 2012) began referring to the Internet as the digital common and cyber security breaches as an analogy to the tragedy discussed by Hardin (1968) in his celebrated article "Tragedy of the commons". Security researchers have characterised the Internet as a common good and information security as a public good (Adar & Huberman, 2000, p.2; Greco & Floridi, 2004; Lukasik, 2011; Powell, 2005; Rosenzweig, 2012, p.8). Public goods are non-rivalrous and non-excludable, i.e., the property of non-rivalrous occurs when the consumption of a public good by one person does not preclude its availability for others to consume. Its non-excludable property does not allow its exclusion from anyone from consuming the good. The natural characteristics of the Internet allows people to come and go freely without being noticed. Unfortunately, this makes users less concerned about contributing to the security aspects of it, which can eventually cause a tragedy of the digital common (Adar & Huberman, 2000, p. 3; Greco & Floridi, 2004, p. 78). Results of an experiment conducted by Adar and Huberman (2000, p.16) suggest that free-riders who do not contribute to the creation of knowledge, are the main culprits of the tragedy which reflects the unavailability of information due to bandwidth congestion.

Since cyber security is a public good where no one can be excluded from its benefits (Johansen, 1977), humans could be the root cause of security breaches. But, they could also prevent the breaches by cooperating towards their implementation of security efforts. Security researchers (Bresz, 2004; Sasse, Brostoff, & Weirich, 2001; Schneier, 2007; Vroom & Von Solms, 2004) identified people as the weakest link in the loop of cyber security breaches in organisations. Security requirements such as policies, guidelines and awareness programmes heavily rely on users' willingness and ability to follow them (Hedström, Karlsson, & Kolkowska, 2013). Thus, users' behaviour for not complying, either intentionally or unintentionally can lead to misuse of information systems that contribute to the breaches (Hedström, Karlsson, & Kolkowska, 2013).

Although several works have subsequently emerged on the tragedy of the internet to reflect Hardin's (1968) work on Tragedy of the Commons, there are limited works exploring cyber security specifically from the perspective of public goods characteristics. Hence, this study is important to understand the relationship between users in the cyber security chain and the characteristics of public goods. With growing number of users in cyber space, it is of utmost significance that some aspects of control are in place to ensure that the continuous expansion of the Internet usage will not be abused (Ponemon Institute, 2014).

1.2 Background of Study

When the Internet was first introduced few conceived the high dependency it will create. While it has transformed the way humans relate to each other it has also brought serious security threats. The recent cyber attack, which spread to 150 countries worldwide (Titcomb & McGoogan, 2017, para 1) showed its potential negative repercussions where the loss was approximately US$4 billion within two weeks of the attack (Berr, 2017). The attack crippled businesses and government entities to demonstrate the weaknesses of the way government and business sectors approach cyber security issues (Carlin, 2017). Among the critical sectors affected were hospitals in the United Kingdom where services were disrupted and data could not be retrieved due to the critical files being encrypted (locked) by "Wannacry", a piece of ransomware that required US$300 worth of ransom in the form of virtual currency bitcoins for the affected files to be unlocked (Curtis, 2017).

Companies leveraging on the Internet to conduct their business by enjoying low cost resources from various parts of the world often overlook security aspects in the supply chain, which can cost a fortune. Although organisations have committed to prevent cyber security breaches through the allocation of resources, these problems still occur. A classic case is the cyber security breach experienced by JP Morgan Chase bank in 2014 despite the bank spending approximately US$200 million each year to protect itself from cyber attacks (Robertson & Riley, 2014). A hacked employee’s password was used to intrude into its systems without the presence of dual factor authentication (Son & Riley, 2014). Without proper awareness and knowledge, users tend to become abusive, opportunists or ignorant when accessing the Internet. These problems contribute to cyber security breaches that affect three main attributes of information, namely, confidentiality, integrity and availability (International Organization for Standardization, 2013; Line, 2013).

1.2.1 Cyber Security in Malaysia

The International Telecommunication Union (ITU) ranked Malaysia third in 2017, in terms of provision of cyber security commitment (International Telecommunications Union, 2017), which was based on legal, technical institutions and frameworks, organisational policy coordination and implementation, capacity building and cooperation in information sharing. However, the increase in global cyber security breaches did not spare Malaysia from cyber security breaches, which experienced an anonymous attack in 2011. In this incident, a hacker group calling itself "Anonymous", attacked a total of 51 Malaysian government websites, causing at least 41 website disruptions (BBC, 2011). The attackers claimed that their actions were due to government restrictions imposed on the Internet (The Malaysian Insider, 2011). This incident has caused organisations to review and improve their security stance in thwarting cyber attacks.

The cyber security landscape in Malaysia can be observed through the incidents reported to MyCERT as presented in Figure 1.1 (CyberSecurity Malaysia, 2018). MyCERT is the main platform for organisations and the public to report cyber security incidents. The statistics show the trend of cyber security incidents reported by individuals and organisations. In Malaysia, reporting cyber security incidents is not mandatory (Bernama, 2015). Although MyCERT has been a platform for cyber security breach reports by organisations and the public, it has been done on a voluntary basis.

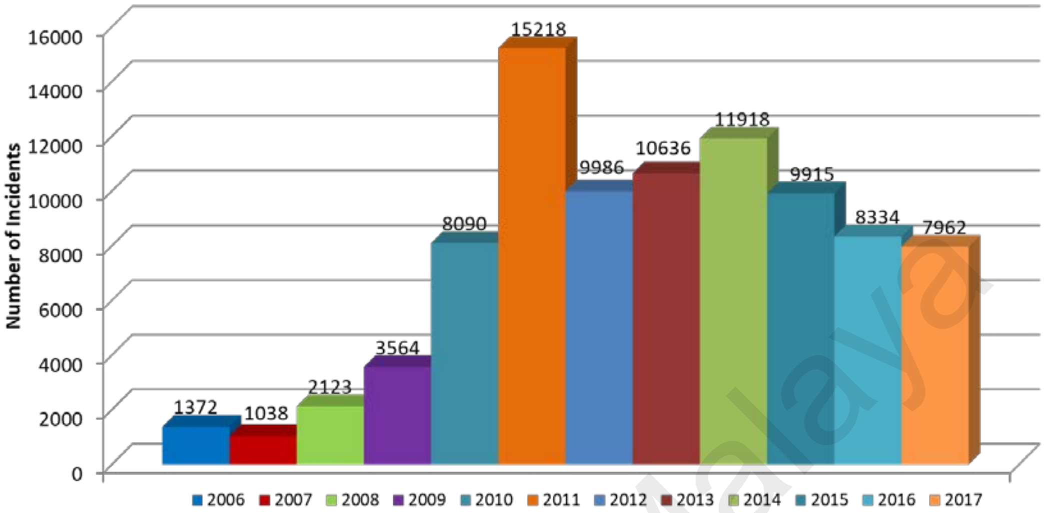


Figure 1.1: Incidents reported to MyCERT, 2006 to 2017
Source: MyCERT (https://www.mycert.org.my)

While in the public sector, its security landscape is measured based on security posture statistics, including security incidents and information security management practices focusing on security processes (Suhazimah Dzazali, Ainin Sulaiman, & Ali Hussein Zolait, 2009). This study also shows that spamming was the most reported security incident (42%) followed by attacks involving malicious codes. In terms of maturity level of information security in the similar sector, statutory bodies seem to be ahead of other organizations followed by federal government agencies in addressing cyber security issues (Suhazimah Dzazali, Ainin Sulaiman, & Ali Hussein Zolait, 2009). Government departments and state departments fell in the medium level. These findings show that ministries seem lag behind other organisations on cyber security issues. Suhazimah Dzazali and Ali Hussein Zolait (2012), asserted that rapid technological changes and more sophisticated attacks could drive more organisations to implement risk management procedures.

In Malaysia, there has been limited studies on cyber security compliance in organisations. Even though they were, these studies were not related to Critical National Information Infrastructure (CNII) sectors (Safa et al., 2015; Safa, Von Solms, & Furnell, 2016). Most CNII sectors related studies on information or cyber security in Malaysia have revolved around national cyber security policy (Shamir b. Hashim, 2011, 2017; Zahri Yunos et al., 2014; Zahri Yunos et al., 2010) and legal aspects of it (Mohamed, 2013; Sonny Zulhuda, 2012). The closest is a study by Noor Ismawati Jaafar and Adnan Ajis (2013) focused only one CNII sector which is the defense sector. This study found that only one organisational factor and three individual factors contributed to security compliance behavior in organisations. Safa, Von Solms, and Furnell (2016), explored attitude towards compliance drawing on respondents from four organisations to study the relationship between employees' involvement, attachment, commitment and personal norms, and attitude in complying with security policy.

1.2.2 Policy Instrumentation for Malaysia’s Critical National Information Infrastructure Sectors

Successful cyber security breaches in one critical sector can have cascading effects on other sectors. Thus, cyber security in CNII sectors needs to be governed and protected. For Malaysia’s CNII sectors, there are three (3) main national policy documents that have been deployed, namely, National Cyber Security Policy (NCSP), National Security Directive No 24 (NSC 24) and a Malaysian Cabinet directive for ISMS Implementation and Certification (MCDISMS). The following sections describe these policy documents in detail.

1.2.2.1 National Cyber Security Policy

The Government of Malaysia has demonstrated its seriousness in protecting its CNII sectors through the formulation of the NCSP where CNII is defined as **“**those assets (real and virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on: national economic strength; national image; national defense and security; government capabilities to function; and public health and safety (Ministry of Science Technology and Innovation, July 2006, p. 3).

Under the NCSP, ten (10) sectors have been identified as CNII sectors: 1) government, 2) defence and security, 3) finance and banking, 4) information and communication, 5) energy, 6) transportation, 7) emergency services, 8) water 9) health services, and 10) food and agriculture (Ministry of Science Technology and Innovation, July 2006). The policy that took effect in 2006 laid down the governance structure and strategic initiatives and plans for CNII organisations to adhere to. The policy has eight thrusts where relevant stakeholders were identified as thrust leaders with defined roles and responsibilities to spearhead initiatives related to the thrusts (Ministry of Science Technology and Innovation, July 2006). As cyber security became part of national security agenda, NCSP was later transferred to the National Security Council Malaysia under the Prime Minister’s Department in 2011 (Shamir b. Hashim, 2017). There are approximately two hundred CNII organisations that were identified by National Security Council (NSC) from the ten sectors (Shamir b. Hashim, 2017) through the sector leads. Sector leads are those institutions identified amongst ministries and regulatory bodies for respective sectors to regulate cyber security related matters in their sectors (National Security Council, 2012). While at the sectoral level, there can be more than one sector lead for each sector, which have been assigned roles and responsibilities to observe and regulate cyber security aspects within their purview. In this context, these institutions play a significant role to ensure regulatory instruments are effective for cyber security compliance within organisations under their purview.

1.2.2.2 National Security Directive No 24

National Security Directive No 24 (NSC24): Policy and Mechanism of the National Cyber Crisis Management is a national policy document issued by the Malaysian Government in providing executive directive for the CNII sectors (Digital News Asia, 2013). It articulates the government's strategy in mitigating cyber crisis and coordinating response through collaboration between public and private sectors so as to provide the mechanism and policy during pre, present and post situation of cyber crisis in CNII sectors. This directive also defines the roles and responsibilities of the three main stakeholders in the ecosystem, i.e., the NSC, sector leads and CNII agencies and/or organisations related to cyber crisis management. In order to avoid operational failures of CNII sectors, all stakeholders are expected to achieve an effective uniformity in monitoring and handling cyber threats in preparation for facing cyber security breaches. Apart from that, this policy document also defines guiding principles to be implemented as national cyber crisis protection mechanisms in the sectors of: first, national cyber crisis management structure; second, national cyber threat level; third, computer emergency response team (CERT); fourth, cyber security protection mechanism, fifth, communication and coordination procedure; and sixth, preparedness programme.

One critical component defined in the NSC24 is the National Cyber Coordination and Command Centre (NC4). The purpose of NC4 is to serve as a centre to coordinate sector leads and CNII organisations in peace and crisis times. It is important to note that at the time this study was completed, NC4 was already established in early 2017 and as such was still in a transition phase. It is not fully functional yet. Thus, the thesis is still good in explaining issues related to the findings of this study where only certain points have so far been resolved.

The ISMS implementation and certification document is a directive that was issued by the Malaysian Cabinet on the 24th of February 2010 for Information Security Management System (ISMS)[3] implementation in CNII organisations in Malaysia (Reference No: *MOSTI*(*R*)/*ICT*/*PSK-1/67* from Ministry of Science, Technology and Innovation (MOSTI)) (Bernama, 2010; CyberSecurity Malaysia, 2013, p. 3). This directive requires all CNII organisations not only to implement ISMS, but also to obtain the certification within three years after the directive takes effect. This directive also requires the relevant sector leads to monitor its implementation which requires the necessary cooperation and coordination at the sector level between sector leads and respective CNII organisations.

1.2.3 Challenges Facing Cyber Security

The main challenge facing cyber security is the increasing attacks, both in number and sophistication, that exploit Internet users who have limited knowledge and awareness of cyber security. The expansion in social networks and mobile usage has attracted cyber criminals targeting users using these platforms. Based on an online survey involving 13,000 online adult users across 24 countries worldwide, it is evident that a significant increase in users accessing the Internet through mobile devices has dragged criminals to the Internet where many respondents confessed to being the victims of mobile, as well as social network platforms (Norton, 2012).

[3] ISMS – Information Security Management System is an international standard that specifies information security requirements based on ISO/IEC 27001. It is a structured security process in managing information security in organisations; either in paper form or in digital form that can be transmitted across the Internet.

It is also reported that the cost of cybercrimes in the United Kingdom is between £18 billion to £27 billion annually (National Audit Office, 2013, p.6). Based on a study conducted by Ponemon Institute (2016, p. 1) on 383 companies in 12 countries, the average total cost of data breach has increased from US$3.79 million in 2015 to US$4 million in 2016, which was mainly caused by malicious attacks. On average, the cost for each lost or stolen record that contained sensitive information increased from US$154 in 2015 to US$158 in 2016 in which it is noticeably higher in regulated sectors due to fines and loss of businesses and customers (Ponemon Institute, 2016, p. 2).

1.3 Problematisation of Cyber Security

The increase in cyber security breaches has raised enormous concerns over the security health of countries. A global survey conducted by Ponemon Institute (2017, p.5) shows an increase of data security breaches at 1.8 % in 2017 compared to 3.2 % in year 2016. The average global cost per lost or stolen record was US$141 where the cost was higher in critical sectors, such as healthcare and financial services than other sectors where the costs reached US$380 and US$245 respectively (Ponemon Institute, 2017, p. 5). Hence, in this report, compliance failure is identified as one of the factors that contributes to the cost of data breach in organisations, indicating that investment on governance of risk and compliance activities are capable of improving organisation's ability to detect the escalation of data breach.

The common view of strengthening information security frequently falls on three fundamental principles; people, process and technology. Previous studies have claimed that the primary cause of successful cyberattacks stem from a lack of technical support comprising of technology and capabilities in managing the technology and related equipment (Deac, 2015). Despite investments made by organizations on security research and implementation of security controls to strengthen security and build organizational resilience, many of them still experience security breaches (Garfinkel, 2012; Ponemon Institute, 2017; PricewaterhouseCoopers, 2012; Thales, 2018). The people aspect has been frequently attributed to the causes of cyber security breaches; in the form of insider threats when employees become disgruntled or when they found increasing security measures were inconvenient that create hurdles for them in performing their tasks (Post & Kagan, 2007).

Based on recent statistics provided by Internet World Stats (2017), the current ratio of world Internet users against world population is almost 50%; where Internet users in Malaysia grew from 3.7 million in 2000 to 24.5 million in mid-2017 with the penetration rate at 78.8%. This is a critical challenge as the number of Internet users have skyrocketed following the deployment of IPV6 addresses mounted with 128 bits depletion to accommodate the depletion of IPv4 addresses that carried 32 bits (Miller, 2015) and also fuelled by Internet of Things (IoT) (Goh Thean Eu, 2015). According to Gartner (2013, para 2), IoT is defined as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment", and this excludes PCs, tablets and smartphones.

Although security researchers have associated cyber security with public goods, there has been limited studies in providing empirical evidence to examine the characteristics of these goods that contribute to security compliance. The main issue with public goods is its free-riding effect that stems from the non-excludability characteristic of the goods (Johansen, 1977). Free-riding leads to unwanted users' behaviour that tend to exploit the goods intentionally or unintentionally. Due to this, certain scholars (Hardin, 1968; Iizuka & Katz, 2010) suggested regulation as a means to control undesired behaviour in groups. In a related study, Albanese and Van Fleet (1985), discovered that free-riding behaviour can be detected in big groups as there is a tendency for members to engage in free-riding in such groups. Previous studies have also indicated that there has been a positive association between a lack of cooperation and participation in free-riding behaviour (Burdett, 2003; Itoh, 1992) where free rider problems entail. Although these studies were based on a different context, their findings concluded that the element of free-riding behaviour can be detected from a lack of cooperation among individuals in the group.

In this thesis, the exploitation of information will damage its value in terms of confidentiality, integrity and availability. Wylder (2003), posited that information security is everyone’s responsibility. Thus, to achieve security compliance, two weaknesses need to be overcome through the cooperation among users. The first weakness addresses the people problem in cyber ecosystem, which is the failure of users to cooperate in achieving cyber security compliance. The second is that, users cannot be excluded from enjoying the benefits of cyber security even though they may not observe the rules of compliance, also referred to as non-excludable characteristic of cyber security. Thus, cooperation is the focus of this study and the problematization of this study is illustrated in Figure 1.2.

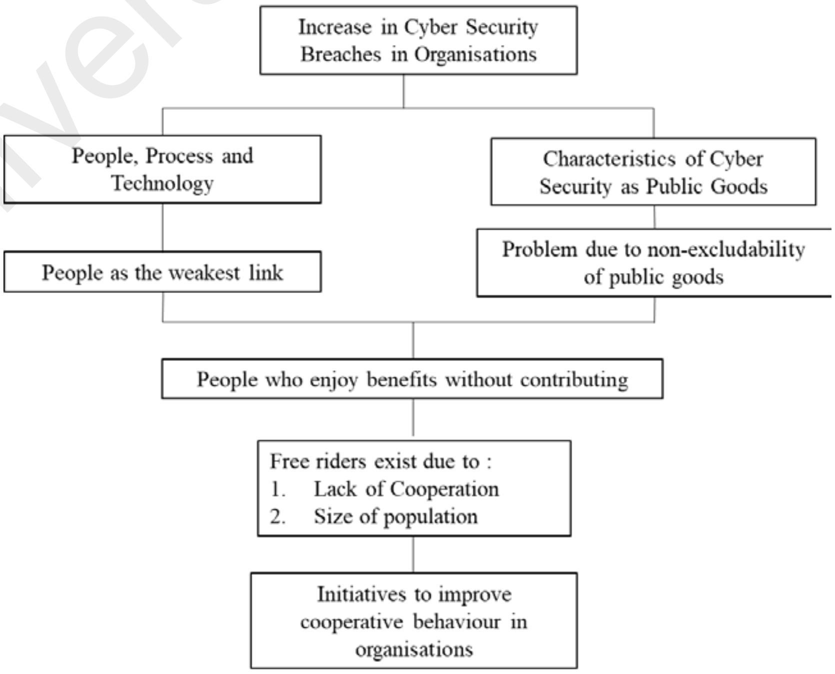

Increase in Cyber Security Breaches in Organisations
People, Process and Technology
Characteristics of Cyber Security as Public Goods
People as the weakest link
Problem due to non-excludability of public goods
People who enjoy benefits without contributing
Free riders exist due to :
1. Lack of Cooperation
2. Size of population
Initiatives to improve cooperative behaviour in organisations

Figure 1.2: Conceptualisation of Problem of Cyber Security
Source: Author

Malaysia has been named as the most cyber-savvy nation as reported by ESET Asia (Ai Lei Tao, 2015). Three factors defined as cyber savvy: one, ability to understand vulnerable online activities, two, risky behaviours, and three, protective measures while being online. However, despite being the most cyber-savvy nation in Asia, consumers in Malaysia did not take right protection measures although they are ranked amongst the top in terms of knowledge of cyber security (Ai Lei Tao, 2015). This could leave Malaysia's cyber environment vulnerable and worse when IoT is pervasively deployed. Based on the National IoT Strategic Roadmap, the implementation of IoT in Malaysia is capable of generating RM9.5 billion to the gross national income by 2020 (Goh Thean Eu, 2015). This suggests that an increase in users through the IoT ecosystem can become a nightmare because most of these devices are developed with IoT capabilities for interaction and communication but without security features to protect information that could affect not only information but also property and human lives.

This study looks at cooperation as a direct and indirect contributor towards achieving security compliance, which is first of its kind in understanding people security behaviour from the aspect of cyber security as public goods. Cooperation is manifested in several ways. It can take various forms and interactions for different purposes, including completing tasks with peers, resolving issues with security vendors and regulatory and compliance matters. However, this thesis focuses on behavioural intention to cooperate amongst users in selected organisations, which may also be applied to the entire cyber ecosystem in Malaysia.

This thesis seeks to argue that without the effective cooperation of the employees of CNII organisations in the cyber ecosystem to achieve cyber security compliance based on the Public goods theory, Malaysia will continuously face cyber threats not only in these organisations but also in the whole ecosystem comprising Small Medium Enterprises

(SME)s, small organisations and home users because the latter do not have sufficient awareness and financial resources and other human and institutional capacity in place. Such a lacking makes it possible for hackers to use these weakness as a platform to continue their cyberattacks. There are several definitions of cyber ecosystem. Due to its simplicity and clarity this study uses cyber ecosystem as defined by Allan (2014, p.1), which refers to “a complex community of interacting devices, networks, people and organizations, and the environment of processes and technologies supporting these interactions”.

1.4 Motivation of study

The extant literature in understanding cyber security problem suggests that cooperation is the key to resolve cyber security issues at the global level, regional and national levels through public and private cooperation. However, these works have hardly touched on the role of cooperation in organisations. Despite acknowledging cyber security as a public good, very little studies have discussed how cooperation can be associated with public goods, and how it can influence organisational practices in achieving security compliance.

A number of studies have emerged consequently to explain compliance in security, among them social bond, threat appeal, and motivation in contributing to security compliance. The main contributions of this study provide a different approach in making users comply with security requirements by analysing the root issue of the public good itself, i.e., cyber security. By identifying the root cause explicitly through its non-excludable characteristic, measures can be formulated not only in organisations but also to shape institutions to provide better measures and governance. Thus, this study is important to understand the relationship between behaviour of users in the cyber security chain and the characteristics of public goods.

While quantitative findings are significant in this study, a qualitative research substantiated with quantitative evidence is important to reveal the real issues on the ground. The qualitative evidence is useful to compliment results and analysis quantified through the statistical methods. This attempt will also unfold the manner with which organisational practices can be used to achieve security compliance. A profound understanding of how cooperation can be induced, and its intervention can raise in management commitment, security processes and security investments is critical to capture institutional change in critical sectors. Given the limitation of resources in protecting organisational assets, it is important to examine how organisations can conduct their practices to achieve compliance.

There has also been limitations in examining institutions that have shaped the roles of important institutional players in managing and governing cyber security in CNII sectors in Malaysia. While there are studies that discuss legal aspects (Sonny Zulhuda, 2012) and policies (Shamir b. Hashim, 2011; Zahri Yunos et al., 2010), such studies have not touched on these issues at the national, sectoral and organisational levels in terms of practices and governance of cyber security ecosystem in Malaysia. Furthermore, existing works have not mapped roles played by institutions in governing cyber security even since the national cyber security policy was launched in 2006 (Shamir b. Hashim, 2017). Little works have linked cyber security in organisations to the role of institutions; sector leads and a central authority in Malaysia, which has become significant especially in the rise of cyber security threats and sophisticated attacks worldwide. This study seeks to elucidate this link by examining the roles of institutions in reflecting effectiveness of rules that have been set in policies and directives at both sector and national levels.

This thesis also intends to demonstrate the association of cyber security with public goods theory by offering scientific value through an empirical study and providing societal contribution to sustain the Internet ecosystem for the country. Using CNII sectors as the focus of this thesis, there are two categories of organisations involved directly or indirectly related to these sectors. The first category is CNII organisations as identified by the National Security Council (Shamir b. Hashim, 2017), while the second category are organisations that are listed as CNII organisations but are regulated by or under the purview of identified CNII organisations that play the role of sector leads for them. For this study, the education sector was included in the second category. There are two main reasons the education sector was included. Firstly, education sector is the sector that consistently produces critical information including researches and intellectual property (IP). Not only a huge amount of funds were allocated to these institutions in doing research, but also to operationalise them. Other than IPs, the image and reputation of universities should also be protected in producing reliable and high quality graduates. Stolen IPs or research value can cost a fortune where the stolen IP estimated by the U.S. Commerce Department is US$250 billion per year (Burgess & Power, 2008). Secondly, there has been no institutions that governed or regulated cyber security matters for the education sector in Malaysia. Since public universities are part of the government responsibilities, MAMPU being the sector lead for the government sector has extended their efforts to govern cyber security in public universities indirectly using the similar governance instruments deployed in the CNII sectors.

1.5 Research Questions and Objectives

The main objective of this thesis is to examine how intention to cooperate, derived from the non-excludable characteristic of cyber security, can mediate organisational security practices in achieving security compliance. This study also analyses the role of institutions in ensuring certain organisational practices are implemented and governed in accordance with national policies and directives.

Based on the research problems identified, using the public goods theory as the foundation of this study, the following three research questions are formulated:

Research Question 1: What are the factors that motivate users to cooperate in achieving cyber security compliance? In answering this research question, four factors that stimulate cooperation are explored: security awareness, security role, technical capability and institutional role. This question raises the need to undertake an in-depth exploration of internal and external factors that stimulate interactions and communications in organisations in obtaining employees' cooperation towards compliance.

Research Question 2: What are the indirect effects of cooperation on the relationship between top management commitment, structured security processes and security investment and cyber security compliance in organisations? This research question suggests the need for an investigation into the mediation effects of employees' cooperation on the relationship between organisational practices and cyber security compliance in organisations. The state of security in an organisation is highly influenced by the way information security is managed and practiced. In answering this research question, the three security practices to be investigated are; top management commitment, structured security processes, and security investment. Top management commitment involves not only providing resources to manage security but also enforcing the security policies and procedures. Structured security processes comprise proactive and reactive processes. A proactive approach includes assessing security risks, threats and vulnerabilities where failure in identifying and managing these security aspects can have adverse effects on organisations. Through such practices, organisations are able to build a secure environment by implementing security measures based on regular assessments. A reactive approach focuses on the way cyber security incidents are addressed and managed in an effective manner. The third aspect of organisational practice revolves around security investment that is made up of competency development and technology deployment.

Research Question 3: Which governance instruments have been effective in regulating cyber security activities in organisations? This question suggests the need to investigate the existing instruments used in regulating cyber security activities in Malaysia, including those governed and regulated at the organisational, sectoral and national levels.

The overall objective of this study is to examine cooperative behaviour in addressing cyber security breaches in selected CNII organisations in Malaysia. In addressing the overall objective of the study, the following are the specific objectives of this study:

Firstly, to investigate the factors that influence employees' intention to cooperate in achieving security compliance. The cooperative behaviour identified in this study stems from the non-excludable characteristic of cyber security as public goods.

Secondly, to analyse the mediation of organisational security practices by users' cooperative behaviour in promoting security compliance that contributes to a secure cyber security ecosystem in organisations. In answering this research question, the effect of "cooperative behaviour" as the mediating variable is explored as to whether the mediation effect is full or partial.

The final research objective is to identify the effectiveness of existing cyber security governance instruments implemented at the organisational, sectoral and national levels in CNII sectors and examine its efficacy in achieving security compliance in organisations.

1.6 Contributions

This research seeks to provide contributions that are deliberated in the final chapter. In summary, the contributions of this research are three-fold. Firstly, at a theoretical level, the findings of this research are targeted at refining existing theories related to public goods and cyber security compliance.

Secondly, this study attempts to identify approaches to inculcate cooperation among employees in organisations to achieve security compliance. The results of the study are also expected to provide a profound understanding of cyber security practices in organisations in Malaysia on how the people factor through employees' intention to cooperate can be strengthened to manage cyber security in organisations. By understanding cooperation in a deeper context, organisations may be able to initiate and deploy mechanisms to boost cooperation not only within organisations, but also with external parties that have linkages with them.

Thirdly, the findings of the research are expected to lead to the identification of more effective instruments to govern cyber security in organisations to better comply with security requirements, which could offer in the desired state of security in CNII sectors. This can minimize the negative impacts on five identified areas; national sovereignty, economic, national image and reputation, government capabilities to function and public health and safety are met (Ministry of Science Technology and Innovation, July 2006).

1.7 Key Concepts

Cyber Security and Information Security

In this study, the terms 'information security' and 'cyber security' are used interchangeably due to the context of its usage. Thus, it is important to understand the difference between the two terms. Information security is defined as "preservation of confidentiality, integrity and availability of information" (International Organization for Standardization, 2014, p. 4) where such information are both in digital and non-digital format. Other information properties that should also be preserved are authentication and non-repudiation where these properties are crucial in dealing with anonymity of users who access the Internet. On the other hand, cyber security is defined as "preservation of confidentiality, integrity and availability of information in the Cyberspace" where Cyberspace is further defined as "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" (International Organization for Standardization, 2012, p. 5). Although information security through the confidentiality, integrity and availability triangle model has been widely accepted as the industry standard, this model needs to be adjusted to suit the rapid evolution of technology and changing of operating environment due to the increased interconnectivities and interoperability.

According to Von Solms and Van Niekerk (2013, p.101) cyber security has a wider perspective than information security where they defined it as “the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace”. They further argued that information and ICT are the underlying cause of potential threats due to vulnerabilities that exist in using ICT as part of the Internet infrastructure. Thus, failing to protect these assets will harm not only organisations but also the public.

Cyber Security Compliance

Security compliance refers to adhering to information security policies and procedures for protecting information in organizations (Von Solms, 2005). Adopting a compliance approach not only satisfies the security requirements of stakeholders but also increases their trust and confidence in aligning information security objectives with organisational objectives. Cyber security compliance ensures that information security mechanisms can work together to effectively protecting the critical information in organizations and ensure that information security is achieved (Herath & Rao, 2009).

In this study, cyber security compliance refers to complying with security requirements comprise of security policies, security procedures, best practices, standards, circular and regulations (Risvold, 2010; Williams, 2001; Wood, 1997) where users need to learn and be aware of these requirements before they can apply them accordingly as they perform their tasks. Although security scholars (Bulgurcu, Cavusoglu, & Benbasat, 2010; Pahnila, Siponen, & Mahmood, 2007; Von Solms, Rossouw & Von Solms, Basie, 2004) emphasized security policies as the prominent instrument for employees to comply with, employees should also adhere to security procedures that are needed to support policies. In addition, organisations need to abide with selected best practices and standards that fit their organisations to ensure security aspects are well implemented and continuously improved. Circulars and regulations which are normally enforced by regulators should also be complied with.

Critical National Information Infrastructure

In Malaysia, the Government of Malaysia has demonstrated its seriousness in protecting its CNII sectors through the formulation of National Cyber Security Policy (NCSP) (Ministry of Science Technology and Innovation, July 2006) where CNII is defined as as **“**those assets (real and virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on: national economic strength; national image; national defense and security; government capabilities to function; and public health and safety (Ministry of Science Technology and Innovation, July 2006, p. 3). Under NCSP, ten (10) sectors have been identified as CNII sectors; 1) government, 2) national defence and security, 3) banking and finance, 4) information and communications, 5) energy, 6) transportation, 7) emergency services, 8) water 9) health services, and 10) food and agriculture (Ministry of Science Technology and Innovation, July 2006).

Institutions

This study uses North's definition where institutions are referred to as the "rules of the game" and firms and organisations as "the players" (North, 1991). In addition, we add North's (1994) "learning processes" that can be applied to improve organisational performance. At the same time, we also acknowledge the fundamental contribution of DiMaggio and Powell (1983) who referred to isomorphism from the perspective of neo-institutional theory to argue that decision-making to drive organisational change can be influenced by three mechanisms, namely: coercive, mimetic, and normative. According to DiMaggio and Powell (1983), coercive refers to regulatory pressure mandated by the government to adopt certain practices in organisations. In describing mimetic mechanism, they explain how organisations tend to model themselves after others when they see positive outcome in them and when they observe uncertainties in their environment. As for normative, DiMaggio and Powell (1983) derived it from formal education and certification not only to perform tasks easier in a similar field but also for better interactions, particularly in resolving issues (DiMaggio & Powell, 1983). Rasiah (2011), extended the meaning of institutions by drawing on Veblen (1915) and Nelson and Winter (1982) emphasizing on a blend of institutions that collectively mould and shape the conduct of socio-economic agents- individuals, firms and organisations. Thus, we use institutions to refer to their roles in shaping security compliance in CNII sectors through their established roles and instruments where these were later internalised in the CNII organisations.

Sector Leads

In CNII sectors in Malaysia, sector leads refer to ministries and regulatory bodies of respective sectors who oversee Malaysia's CNII agencies and organisations (National Security Council, 2012). Depending on roles and functions, they were appointed by the regulatory powers of the CNII agency and/or organisation thereunder. Among others, their roles include all aspects of cyber security activities and initiatives as defined in the National Security Directive No. 24 (National Security Council, 2012). Several sector leads are entities that provide rules and regulations for organisations to follow.

Tasks Interdependence

According to Wageman (1995), processes act as one of the sources from where interdependence among members in organisations can be derived in which members execute the work. In narrowing it further, task interdependence requires members in a group to work interdependently where each member complete his or her part of the whole task. As posited by Kiggundu (1981), task interdependence comprises three domains: scope, resources and criticality, whereby scope describes how a particular job in a unit is interconnected with other units. Resources describe the degree of involvement of interdependence in giving and receiving resources in performing the job while criticality is the extent of significance of interdependence between the focal job and other jobs and on how the performance of the focal job becomes dependent on the performance of other interdependent jobs (Kiggundu, 1981).

Previous literature have discussed various views of task interdependence that require associate actions to be done interdependently amongst group members for tasks completion (Wageman, 1995). Thomson's view of tasks interdependence (as cited in Wageman, 1995, p. 146) was derived from the technology available in completing the whole task where sub-tasks are performed in sequence order such as in the manufacturing environment. Scott, Bishop, and Chen (2003) posited that task interdependence has a direct relationship with willingness to cooperate; where workers must cooperate among themselves to efficiently perform tasks that require interdependence.

Task interdependence exists in a group whereby, members seeking to deliver their respective tasks, need to share resources to meet desired outcomes (Cummings, 1978). In other words, task interdependence forms the backbone of relationships among members in groups where task interdependence increases along with its difficulties (Van Der Vegt, Emans, & Van De Vliert, 1999).

1.8 Thesis Outline

This thesis is structured as follows. Chapter 1 provides the introduction, which includes the background of study, problem statement, motivation of study, research questions and objectives, research contributions and key concepts. Chapter 2, presents the literature review, which consists of a profound review of related works done related to this study. Chapter 3, discusses the research methodology that will be used which includes the analytical framework and the methods for data collection and analysis. Chapter 4, analyses findings and discussion related to research question 1 on the factors associated with the behavioural intention of employees to cooperate in achieving security compliance. Chapter 5, evaluates the findings and discussion related to research question 2 on the mediation effects of cooperation on cyber security practices; top management commitment, structured security processes, security investment and cyber security compliance. Chapter 6, examines the effectiveness of cyber security governance instruments of compliance implemented at three levels; organisational, sectoral and national level. Chapter 7, presents the summary and conclusions, which include implications for theory, policy and practices, as well as suggestions for future research.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Cyber security breaches have become a major concern in many organisations especially in critical national infrastructures as the attacks on one sector have major devastating impacts on the other sectors which will eventually affect public safety. The rapid expansion of technology in connecting people globally indicate increasing users on any device/s by many folds. This has caused serious problems in the chain of security. Previous studies related to information security compliance were limited to only one level that is at the organisational level. In this study, three aspects are addressed. First, the behavioural factors that influence cooperative behaviour in organisations; second, the organisational practices that drive cyber security compliance in organisation; and finally governance of cyber security at the three levels. The three levels addressed are the organisational level, the sectoral level and the national level. Organisational level refers to selected organisations as discussed in sub-section 1.4; the sectoral level refers to the CNII organisations that play a regulatory role in their sectors pertaining to cyber security; and the national level refers to the National Security Council that has the mandate to govern cyber security for all the CNII sectors in Malaysia.

Thus, using the dominant public good and institutional theories, this study investigate further the sector leads of the ten CNII sectors and central authority level, the National Security Council, as the institutions responsible for governing cyber security in the CNII sectors in Malaysia.

The literature review in section 2 is separated into three sub-sections, namely, sub-section 2.1 deals with the introduction; sub-section 2.2 reviews the theoretical framework and evidence and sub-section 2.3 reviews empirical evidence. In sub-section 2.2, the following theories were reviewed:

- the theory of public goods,
- the theory of planned behaviour,
- the theory of cooperation,
- the theory of institutions including isomorphism, and
- power distance.

Sub-section 2.3 presents empirical evidence where previous studies are reviewed to establish the variables used to answer the three research questions as stated in sub-section 1.5. The literature review for the theories for research question 1, are addressed in sub-sections 2.2.2 to 2.2.5. The variables for research question 1 are addressed in sub-sections 2.3.2 to 2.3.5 and 2.3.10. The literature review for research question 2 are found in sub-sections 2.2.4 and 2.2.5 for the theories and in sub-sections 2.3.7 to 2.3.9 for the variables. As for the third research question, the theories are addressed in sub-sections 2.2.5 and 2.2.6 while the variables are addressed in sub-sections 2.3.11.1 to 2.3.11.4.

2.2 Theory and Evidence

The Internet has introduced a new model to deploy security practices in organisations. Although being compliant with security requirements does not provide assurance for security breaches not to occur, it is capable of minimising risks of breaches through preventive measures. Thus, organisational practices need to be consistently revisited and reviewed to ensure compliance is met. In this study, cooperation in organisations is presented as an effective approach to achieve security compliance.

2.2.1 Economics of Information Security

With the increase of cyber security incidents on the Internet, security researchers have been associating economics principles in identifying possible solutions (Anderson, 2001; Anderson & Moore, 2006; Schneier, 2007). These issues relate to information security problems which include public goods (Adar & Huberman, 2000; Greco & Floridi, 2004;

Rosenzweig, 2012), free-riding (Adar & Huberman, 2000), externalities, misaligned incentives and asymmetric information (Anderson, 2001; Moore, 2010).

2.2.1.1 Information Security In The Economics Discipline

Anderson (2001), is one of the early security researchers who looked at the issue of information security from the economic perspective. He put a contradictory view of information security where the reasoning of a state of insecurity can be better explained through microeconomics principles. By focusing on technical aspects in resolving security incidents, the non-technical issues were neglected. The state of information insecurity is described as a situation where information security breaches occur against security policies or failure of controls which affect the system, service or network.

2.2.1.2 Misaligned Incentive

Anderson and Moore (2006), stated that systems are likely to fail when the person who guards them is not the person who suffers when the systems fail. They referred to this situation as misaligned incentives where those who are responsible in protecting the systems have no incentives in ensuring they are safe and secure. Varian (2000), suggested looking at two neglected areas: the lack of awareness of computer users of the security threats posed by cyber attackers and the lack of incentives to avoid information security abuse by the respective organisations. Varian (2000), further stated that liability should be assigned to the party that best managed the risk, be it the computer-user or the computer ecosystem of that organisation, because they were aware of the extent of weaknesses and controls that were in place. By saying this, Varian (2000) further emphasized the importance of aligning incentives, so the party that is liable would do the necessary in managing the associated risks. In taking an example of computer users who were not aware that their machines were being used as a launching pad to attack others, Varian (2000) believed that the service provider is more accountable for the attack on the basis that broadband users normally have no idea that their machines were taken over by attackers.

2.2.1.3 Externalities

Cyber security generally creates positive or negative externalities in its ecosystems. According to Camp and Wolfram (2000, p.1) "economists define externalities as instances where an individual or firm’s actions have economic consequences for others for which there is no compensation". Negative externalities have been frequently discussed in security literature (Anderson & Moore, 2006; Schneier, 2007). Schneier (2007), pointed out that externalities that exist in the software industry have actually caused the emergence of insecure software in the market that directly impacts users. The reluctance of security vendors to further invest in making software more secure for users has led the costs of its failure, such as patching cost where monetary and non-monetary loss due to security breaches to be passed down to users (Schneier, 2007). In other words, users of insecure software have to bear the impacts of the decision made by these reluctant software vendors in securing their products. In reducing the burden to the users who pick up all the relevant costs of security, Schneier (2007) suggested that fixing the cost of insecure problems to be the responsibility of the security software vendors or developers. However, Anderson and Moore (2006) were of the view that misaligned incentives, such as compensating the wrong parties, drive the dominance of insecure softwares in the market as software developers were not compensated for the costs involved in strengthening the security features of the software.

2.2.2 Theory of Public Goods

Economic scholars have been classifying goods based on rivalrous and excludable attributes. A good is described as rivalrous when its consumption by a person creates a rival because his/her consumption prevents others from consuming it. The goods become non-rivalrous when an additional person can consume the good without reducing the benefits of other consumers. Goods are described as excludable when there is a possibility of limiting or excluding others from its consumption (Rosenzweig, 2012; Solum, 2010), and becomes non-excludable when a person (who is not paying for consuming the good) cannot be excluded from consuming it; thus enjoying the benefits of it. Various consumption goods have been categorised based on these attributes.

The distinction between the concept of public and private goods stems from the work of Samuelson (1954) on the basis of non-rivalry consumption. Musgrave's further suggestion to add the "exclusion" attribute in defining goods (as cited in Apesteguia & Maier-Rigaud, 2006, p. 647) has resulted in common pool resources goods and club goods. Common pool goods are characterized as having rivalrous and non-excludable attributes which are frequently associated with congestion (Rosenzweig, 2012; Solum, 2010). Club goods are characterized as having the excludable and non-rivalrous attributes except that Solum (2010, p.824) described it as non-rivalrous until it reaches a certain threshold, where additional consumption causes the goods become rivalrous, for example, the highway toll where an access fee is charged to motorists to access the highway. Common goods, also known as common pool resources, are non-rivalrous but difficult to exclude due to its nature where people share the goods and consume the goods freely. However, efforts must be made to sustain it (Deneulin & Townsend, 2007). Although cyberspace apparently has public good characteristics where its architecture is inherently non-excludable and non-rivalrous, services available on this architecture do not have the same characteristics (Kaul, Grungberg, & Stern, 1999).

From the perspective of cyber security a public good, people are the weakest link as this good is non-excludable and non-rivalrous (Adar & Huberman, 2000; Greco & Floridi, 2004; Powell, 2005; Rosenzweig, 2012). The prominent characteristic of a public good, which is non-excludable to users provoke people to consume goods without paying for it, and non-rivalrous, which allows people to continue consuming the same good without additional costs (Anderson, 2001; Rosenzweig, 2012; Solum, 2010; Stigler, 1974). The two features make the benefits of sharing the good for the benefit of society as a whole will be the best if the conduct is good (e.g. productive knowledge sharing) and worst (e.g. crime that undermines society) if the conduct is bad. However, its non-excludable attribute exposes the goods to free-riding which is known as "failure of collective action" where benefits of the goods will be enjoyed by all although not all contribute to it, that is the burden of protecting the good (Deneulin & Townsend, 2007; Johansen, 1977).

When a resource is held in a common that is accessible to all, there will be persons who will grab the opportunity in ripping off the benefits of the resource while spreading the costs amongst others (Hardin, 1968). Worst still abusers of public goods often leave behind a trail of damage that can destroy the provision of such goods. On the one hand, the negative effect arises from legally right conduct. For example, Gordon, Loeb, and Lucyshyn (2003) argued that free-riders can negatively affect the state of information security by causing security expenditures to be under-invested by some firms. The under-investment was due to reliance of firms on security investments made by others. When this situation is continuously allowed without appropriate measures in place, the state of security will be eventually compromised.

Given the arguments above, public goods, such as national security, and knowledge should not be left to markets. Both their delivery and their consequences entail collective actions by users who benefit from their provision.

2.2.2.1 Cyber Security as Economics Good

Due to its attributes, public goods are normally not charged for being accessed or consumed, thus the producer is not able to get the benefits of the goods (by charging them) which gradually creates the goods to be underprovided (Lant, Ruhl, & Kraft, 2008). Some public goods cannot stay public due to their continuous usage where too many people using the public goods will result in the good becoming saturated, thus gradually reducing its non-rivalrous attribute. If Internet is considered as a public good by many researchers, there should not be any issue as to whether Internet users should be charged proportionately according to their access. However, a work produced by Huberman and Lukose (1997) has demonstrated otherwise. Referring to the Internet as a public good, the Internet users tend to greedily use the Internet without realizing the consequences on the whole of Internet performance due to their actions. This is the effect when Internet users are not charged proportionately for the Internet access, thus subsequently resulting in unnecessary congestion.

There have been discussions in literature whether cyber security has been sufficiently provided to the users. Although the provision of public goods is the responsibility of the state as claimed by several researchers, Deneulin and Townsend (2007) argued that the national government is not the only actor for this provision. From the context of cyber security, according to policymakers, the government cannot provide it sufficiently without cooperation from the private sectors (Böhme, 2006; Powell, 2005). Powell (2005), claimed that cyber security is underprovided in the private sector where users who secure their computers do not benefit from their security deployment, instead it creates positive externalities that accrue to others. These spill-over benefits can reduce the probability of other users (who do not secure their machines) of being attacked through owners who have deployed necessary security measures. This creates a scenario where users who are capable of providing security will not do it just because they will not directly benefit from the deployment. Thus, cyber security is being underprovided.

Although information security has always been regarded as public goods, Rosenzweig (2012), argued that not all aspects of security services fall under the public goods domain, instead they fall under different categories depending on their functions and purposes. For an example; information on threats and vulnerabilities are public goods and implementation of security defence tools in organisations are categorized as private goods (Rosenzweig, 2012, p. 8).

2.2.2.2 Tragedy of the Commons and Tragedy in the Digital Environment

Using a pasture as the commons in his article, Hardin (1968, p.162) described how an individual who maximised his gain by consuming too much shared resources could cause a tragedy. For Hardin (1968), regulation was the possible answer to this social dilemma. Security scholars have made various references in connecting the issue of Internet usage to the tragedy referred by Hardin (1968). Hardin (1968), argued that when many users use a scarce resource, it can degrade the environment; thus leading to a tragedy. The notable difference between the two environments is that the commons referred to by Hardin (1968) is natural resources-based whereas the Internet is man-made. Greco and Floridi (2004), referred the Internet as a public good with a borderless environment compared to bounded environment presented by Hardin (1968). In discussing of two types of agents that destroy the common resources, firstly, Hurwitz et al. (2012) referred hackers, spammers, cyber activists and those are similar as parasites where they cause nuisance to others. Secondly, another type of destroying agent comprises stakeholders, such as governments, online service providers that go beyond limitation in pursuing their own interest. These agents have no intention to damage these resources, but their actions somehow reduce public trust in using those resources. In referring to a study by Adar and

Huberman (2000), Greco and Floridi (2004) concluded that the work by Adar and Huberman (2000) was not explained in the context of the tragedy discussed by Hardin (1968), instead it was due to lack of improvement on the Internet.

Interpreting the Tragedy of the Commons model by Hardin (1968), Greco and Floridi (2004) argued that increasing ICT users to bridge the digital divide without making them responsible of their own actions can cause exploitation. In this context, the exploitation refers to the congestion of network bandwidth due to the selfish attitude of users and information pollution, such as spam; in which these two situations gradually contribute to tragedy in digital commons. Almost all works produced related to tragedy in the digital world focus the aspect of availability of information, where congestion leads to performance degradation (Greco & Floridi, 2004; Huberman & Lukose, 1997). Apart from availability, other two critical aspects of information which are confidentiality and integrity were not discussed in these literature. Impact on unavailability of information or online services disrupts business services where the longer the disruption, the more the damage to the organisations. Impacts on compromised integrity and confidentiality of information is no less. Thus, these three properties of information should be preserved in order to achieve information security in organisations (International Organization for Standardization, 2013). In this context, tragedy on the Internet should not be limited to the availability factor but also includes leakage of its confidentiality as well as compromised integrity of the information.

2.2.2.3 Free-Riding and Collective Action

Free-riding theory has been central to the degree of excludability of goods; between public and private goods. The problem of free-riding arises due to the non-excludability characteristic of public goods that allows all including individuals who do not contribute to enjoy the benefits that public goods can offer. Adar and Huberman (2000), suggests that continuous free-riding by excessive free-riders (who are not charged on using a public good) in the Gnutella system degraded the performance of the file-sharing environment. Rosenzweig (2012), refers free-riders as individuals who want to enjoy the benefits of a public good but refuse to contribute to it. Somehow, they expect others will do so even in the absence of their participation.

According to Olson (1965), rational behaviour of people in minimizing cost relative to benefits gained from public goods can affect groups productivity. Albanese and Van Fleet (1985), postulated that there are two types of free-riding relative to provision of public goods; weak free-rider hypothesis that creates sub-optimal public goods (Samuelson, 1954) and strong free-rider hypothesis that does not create the provision of public good due to large groups (Brubaker, 1975). As for the latter, Albanese and Van Fleet (1985) suggested that increasing a group’s size creates potential free riders unless coercive or special incentives are in place to control this. Brubaker (1975), was in a different view where he suggested that individuals may reciprocate and commit when they are assured that the others will do the same. Meanwhile, Johansen (1977), argued that the tendency to free-ride is a basic human nature. Individuals tend to contribute in a public good when there is a certain level of assurance that other members in the group will also contribute appropriately for the provision of the good (Brubaker, 1975; Johansen, 1977) .

Free-riding has been referred to by many scholars when there is absence of contribution of public goods by individuals although they will not be excluded from enjoying the benefits the public goods have to offer. Olson (1965) and Hardin (1968) have created wide acceptance of the proposition of free-riding towards the provision of public goods. However, economic scholars argued that their arguments were solely on theory; thus leading researchers to conduct experiments in conforming their theoretical arguments (Brubaker, 1975; Marwell & Ames, 1981; Schneider & Pommerehne, 1981). Through an experiment conducted by Schneider and Pommerehne (1981), free-riding cannot be presumed to happen as concluded in previous studies; but people only free ride in a particular situation when they have the opportunity to do so. Using a textbook as a public good in an experiment, Schneider and Pommerehne (1981) discovered that free-riding behaviour exist at a moderate level, where incentives can influence the behaviour of individuals. The tendency to free-ride is higher on consumption goods rather than any other public goods. Upon critically examined previous literature, Schneider and Pommerehne (1981), found that Brubaker's (1975) discussion emphasized only on the significance of free riding without exploring motivations that could possibly lead to a more collective behaviour among individuals.

Free-riding has also been associated with collective actions where it occurs when individuals fail to participate in activities that can collectively benefit the group; either through coercion or appropriate incentives (Stigler, 1974). The non-exclusivity of public goods triggered the rationale for individuals not to contribute voluntarily when they can still gain the benefits even without contributing. Participation has also been identified by certain scholars as one of the important factors for collective actions to succeed where Stigler (1974) emphasised that there is a tendency on the reduction of the benefits to be gained from collective actions if a member in the group does not participate and cooperate. Thus, the probability of collective action to happen depends on the strength of each individual that participates in the group. The free-riding problem has also been frequently associated with a lack of enforcement (Canadian Council of Ministers of the Environment, 2013).

The effect of free-riding activities is also felt in other contexts of adverse effect of information security. Anderson (2001, p.358) asserted that users’ reluctance to invest in preventing their systems from being exploited in attacking others compared to how they are willing to spend money in protecting their own computer can have adverse effects if other users adopt this behaviour. Schneier (2007) further argued that software providers do not invest much in incorporating security in their products, where the cost of breaches due to software failures were passed down to users. In a similar context, Gal-Or and Ghose (2004), furnished the evidence of the possible existence of free-riding activities which is based on cost reduction spill-over effect. Based on their study, the disclosure of vulnerabilities information in a particular technology had a cost-saving spill-over effect on the other firm, where less investment will be made by the other firm for the similar technologies deployed in organisations.

2.2.2.4 Self-Regulation in the Common

In dealing with congestion discussed by Hardin (1968), Ostrom (1990) disagreed with the economists' view that when an individual's property right in commons is absent, the resources will be exploited; thus only privatization can be the possible solution to this over-consumption problem. Ostrom (1990) explored how common pool resources together with its administrative cost could be organised efficiently. However, Hurwitz et al. (2012) argued that in the context of cyber space, the work produced by Ostrom (1990) on self-regulation in the commons is hardly applicable in sustaining the cyberspace due to the current state of cyber space and the users' behaviours**.**

2.2.3 Theory of Planned Behaviour

Theory of planned behaviour (TPB) has been widely used in various studies to predict a behaviour of interest. The theory postulates that behavioural intention can be explained by attitude, subjective norm and perceived behavioural control (Ajzen, 1991). Attitude refers to feelings by individuals towards a behaviour of interest that can be positive or negative while subjective norm leads to social pressure on individuals either to perform or not to perform such behaviour (Ajzen, 1991, p. 188). In relation to perceived behavioural control (PBC), Ajzen (1991, p. 183) refers to individuals' perception of the ease or difficulty to perform such behaviour. Perceived ease and difficulties to achieve the behaviour of interest will be affected by conditions that facilitate the availability of resources and opportunities to perform such behaviour (Ajzen, 1991). Bandura (1977,1980) as cited by Ajzen (1991, p. 183), argued that availability of resources and opportunities affect the confidence level for people to perform the behaviour of interest.

TPB posits that behavioural intentions are immediate antecedents to actual behaviour. Behavioural intentions are a function of salient beliefs that affect intentions and actual behaviour through attitudes and subjective norms. Based on TPB, behavioural intention can turn into actual behaviour only if the behaviour in question is under volitional control. It is under this condition that a person can decide to perform the questioned behaviour willingly or not (Ajzen, 1991, p. 182). On the contrary, when the behaviour of interest is not entirely under the volitional control or when individuals are in a situation where they are no longer capable of controlling their behaviour, TPB predicts it by incorporating perceived PBC. In short, PBC becomes important when volitional controls diminish (Ajzen, 1991).

2.2.4 Cooperation

Smith, Carroll, and Ashford (1995), posited that cooperation is generally viewed by others as a platform which physical interactions is necessary in establishing relationships among individuals, groups and organisations for mutual benefits. However, in situations where individuals are more concerned in pursuing self-interest, these selfish behaviour can lead to failure for all in the group (Axelrod, 1984). Smith, Carroll, and Ashford (1995), further added that cooperation can be formed vertically through engagement of different level of groups in organisations as well as horizontally between them and with external parties. Cooperation is established when organisations put commitment in terms of efforts, resources and time to meet objectives that benefit the organisations (De Cremer & Van Knippenberg, 2002). Upon critically examined forty six articles related to cooperation, one important finding established by Smith, Carroll, and Ashford (1995) links to this study which is cooperation as a performance indicator.

In order to understand the cooperative efforts in a hierarchical form between a superior and subordinates in organisations, Itoh (1992) deliberated two types of cooperation; induced cooperation and delegated cooperation. The former was described as cooperation that is motivated by a monetary incentive for an agent to help each other through a grand contract (Itoh, 1992, p. 3). This type cooperation can be optimal where subordinates are less risk averse or when there are similarities in performance measurement and costs involvement while performing their tasks. However, the latter emphasizes on delegation by a superior to his/her subordinates to arrange themselves towards cooperation while performing their tasks which tend to resolve the free riding problem (Itoh, 1992, p. 6). Delegated cooperation is attained when subordinates who are more homogeneous in certain ways, such as risk attitudes, are jointly responsible to perform their tasks. It was also observed that induced cooperation can be transformed into delegated cooperation when subordinates monitor each other and coordinate among themselves (Itoh, 1992, p. 18).

Benefits of cooperation can be understood through the "prisoner's dilemma" where two rational individuals chose not to cooperate when there is lack of opportunity to initiate cooperation (Axelrod, 1984; Killingback & Doebeli, 2002; Trivers, 1971). Cooperation gained through reciprocal altruism is not easily exploited by individuals (Axelrod, 1984; Killingback & Doebeli, 2002). Trivers (1971), had advanced the reciprocal cooperation theory to explain how actors and recipients give and receive in an alternate manner. In understanding cooperative behaviour among living organisms, Melis and Semmann

(2010) were of the view that cooperative behaviour can also control free-riding behaviour apart from collectively working towards a common goal. In its broader sense, cooperation "provides a benefit to another individual (recipient) or are beneficial to both the actor and the recipient" (Melis & Semmann, 2010, p. 2663). However, Wageman (1995) argued that free riding only give benefits personally to individuals that can eventually cause failure in achieving cooperation.

2.2.4.1 Evolution of Cooperation

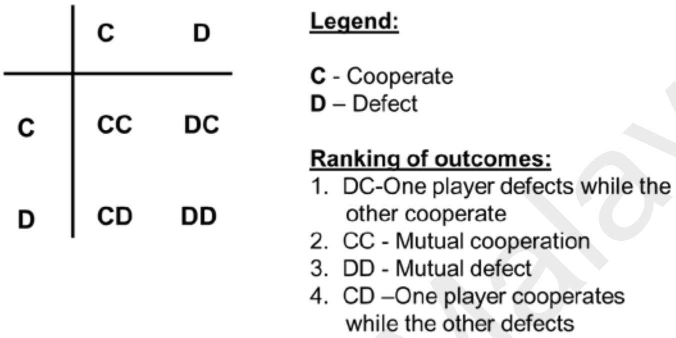
The evolution of cooperative behaviour has been discussed in a book by Axelrod (1984), where he presented the Theory of Cooperation. This theory is based on individuals who pursue their own self-interest in the absence of coercive actions by the central authority in getting them to cooperate with each other. Using two industrial nations that imposed trade barriers on each other's exports as an analogy to understand the fundamental tenet of cooperation, Axelrod (1984; p. 7) asserted that the basic problem in cooperation was when "the pursuit of self-interest by each leads to a poor outcome for all."

In referring to cooperative behaviour in biological systems discussed by Hamilton (1964), Axelrod (1984) posited that cooperation which is based on reciprocity can be stable in the biological world under suitable conditions. In biological systems, cooperation can occur when members in the system are not related and not even able to appreciate the outcome of their own behaviour (Hamilton, 1964). An example of such behaviour was captured in Waloff's discussion on ants "Lasius flavus and L.niger" (as cited in Hamilton, 1964, p. 44). Here, there were two situations that led to the success of the establishment of the nest chamber for the queen in the ant colony. These were queen ants who did not have a close relationship with each other. They could either fight among themselves or cooperate together in establishing the initial nest chamber. In either case, only one queen ant is allowed to survive and use the nest. Thus, Hamilton (1964) argued that the chance for a queen ant to succeed to use the nest is higher when they cooperate to dig the ground to make the nest chamber rather than when the queen ant had to do it alone through fighting.

Killingback and Doebeli (2002), suggested that cooperation needs to be understood from two aspects; cooperation between related individuals who have genetic association referred to as “kin selection” and those who are non-related individuals. In explaining cooperation amongst relatives, Killingback and Doebeli (2002) posited that if they interact with each other, they are capable of increasing the frequency of altruistic traits. But, for those who are non-relative, Killingback and Doebeli (2002) viewed reciprocal altruism as one of the possible explanations of cooperation. To encourage cooperation in organisations, relationships among members in the organisations should be structured for them to have frequent and durable interactions (Axelrod, 1984). Axelrod (1984), has also used the case of insurance in shipping business to explain the importance of frequency of interactions that resulted in the establishment of Lloyd's of London. This organisation was the outcome of frequent interactions of independent insurance brokers that traded with each other in pooling their business risk.

2.2.4.2 Prisoner’s Dilemma and Cooperation

As discussed earlier in this section, the problem with cooperation is when self-pursuing individuals cooperate without having full concerns of the welfare of others as the whole. Previous related studies have associated the cooperation problem with the "prisoner's dilemma" (Axelrod, 1984; Killingback & Doebeli, 2002; Trivers, 1971). Prisoner’s dilemma is a concept based on a game theory that reasoned out why two rational individuals opt not to cooperate although both would benefit by cooperation. Using a symmetric game of two players in describing this dilemma, there are two possible strategies for players; either to cooperate (C) or to defect (D). The payoff of the game is illustrated in Figure 2.1 with four possible outcomes; the best possible outcome is when a player defects while the other cooperates (DC) and the worst is when one player cooperates as the other defects (CD). The second best outcome is when both cooperate (CC) followed by both players defect (DD). Based on this game, a player would get a better payoff if he betrays the other. However, there will be a reward for mutual cooperation if both cooperate, and punishment for both players if both defect.



	C	D
C	CC	DC
D	CD	DD

Legend:

C - Cooperate
D – Defect

Ranking of outcomes:

1. DC-One player defects while the other cooperate
2. CC - Mutual cooperation
3. DD - Mutual defect
4. CD –One player cooperates while the other defects

Figure 2.1: Payoff Matrix for the Prisoner's Dilemma
Source:(Kollock, 1998)

Killingback and Doebeli (2002), argued on the limitation in using the prisoner's dilemma as a model of cooperation as it has only two possible options; to cooperate or defect where both of which are rigid. The nature of cooperation requires more players; thus cooperation should be continuous in allowing a certain degree of cooperation to exist (Killingback & Doebeli, 2002). Due to this limitation, Killingback and Doebeli (2002) have extended the prisoner's dilemma by incorporating continuous cooperation via reciprocal altruism. However, Trivers (1971), had earlier introduced reciprocal cooperation theory where actors and recipients give and receive in an alternate manner. This theory describes how people reciprocate upon receiving help instead of exploiting them by not returning the favour.

2.2.4.3 Challenges in Cooperation

According to Melis and Semmann (2010), the challenge of cooperative behaviour amongst humans is not only getting them to cooperate but in controlling those who free-ride. Lovine and Tyson’s observation on free riding (as cited in Itoh, 1992, p. 6), suggested that teams that are grouped in accordance to interdependence tasks tend to co-organise their work together for a mutual gain. It was also observed that costs incurred by free riders (who deviate from cooperative work norm) had to be shared by the rest resulting in social sanctions to be imposed.

While organisations are urged to promote cooperation to allow a quick adaptation to changes in organisational environment such as innovative changes in the Internet era (Schalk & Curşeu, 2010). Melis and Semmann (2010) argued that cooperative behaviour between actors and recipients does not only exist between those who know each other but also between strangers. This behaviour has grown amongst humans to not only cooperate but also to regulate free-riding. Various mechanisms have been deployed to ensure cooperation is strengthened whilst free-riding is deterred, that include reward and punishment. Past empirical studies indicate that there is an inverse association between cooperation and free-riding behaviour (Burdett, 2003; Itoh, 1992). Although these studies are not in the context of cyber security, their findings show that free-riding behaviour is positively associated with a lack of cooperation among individuals in groups. In a similar study by Burdett (2003) on a group assignment amongst university students, dissatisfaction with certain individuals who underperformed, had undermined cooperation among them, thus affected the overall group performance.

Alchian and Demsetz (1972) asserted that cooperative behaviour instilled through teamwork is able to gain better output than the summed output by individuals’ work. Alchian and Demsetz (1972), further emphasized two important factors in producing teamwork; first, the different types of resources used in producing it and second; the outputs produced should not be based on separate outputs that were summed together; instead there should be outputs as the outcome of the teamwork itself.

Thus, we draw on these findings by Alchian and Demsetz (1972), to analyse how cooperation mediates between organisational practices and cyber security compliance in organizations in Malaysia.

2.2.5 Institutional Theory

In this thesis, North’s (1991) definition of institutions as the "rules of the game" and organisations as the "players" are used to define rules for societies and economies to enforce them in a formal or informal manner. Institutions were designed by human beings to create order and reduce uncertainties in order to form political, economic and social interaction structures through formal and informal constraints (North, 1991). This means that organisations as players are bound by the rules set by the institutions. Formal constraints include those specified in contracts, laws and constitutions while informal constraints include sanctions, taboos and norms of behaviours. In relation to social interaction as one of the areas examined in this study, the foundation of it can be understood from the perspective of a game theory. North (1991, p. 97; 1994, p. 6), argued that cooperation can only be achieved among individuals when three conditions are met in a game, first when the game is repeated, second, when complete information of player’s past performance are obtained and third, when the number of players are small. Thus, it is a complicated process in forming up institutions that able to balance off between benefits and cost with cooperation since it also demands political supports (North, 1994).

The evolution of institution is shaped by time through learning process of human beings, where time is related to societal change and economic performance North (1994). In the process of the institutional change, North (1994) identified learning as a long term source of change in organisations where it is fundamental for organisations to survive. North (1994), further argued that throughout the process, individuals in societies acquire knowledge by taking into account current and previous learning and experiences which are capable of influencing them in making choices.

In public goods literature, the role of institutions in avoiding abusive players were widely discussed. Similar to cyber security, institutional role in nation states is increasingly important to protect its users as well as secure its cyber space. Farrell and Knight (2003), deliberated on how institutional change occurs when those who are in a greater power position are capable of making changes. In a situation that involves the element of trust such as cyber security, the impact of this institutional change can be huge. When trust is lost between actors, this will eventually affect cooperation amongst them. In circumstances that are complex such as the existence of heterogeneity, institutions play mediating roles especially on non-linear relationship between group size and collective action (Poteete & Ostrom, 2004).

Although often overlooked by mainstream economists, Veblen (1915) had argued over the social origin of institutions. This argument that rightly classified human as social rather than economic argument offers a powerful platform for building cooperation. Since the focus of individuals in establishing cooperation is largely targeted at eliminating economic losses, we take on Rasiah's (2011) reference to humans as socioeconomic agents seeking to optimise outcomes in a largely imperfect world. Nelson and Winter (1982) had succinctly built on Veblen's (1915) exposition of the evolutionary coordinates of institutions and institutional change. Rasiah (2011), extended this logic referring to a blend of institutions working collectively to shape the conduct of industrial socioeconomic agents individuals, firms and organisations. Firms and organisations exist to solve collective action problems. Elements of cooperation to compete collectively was also advanced by the industrial district exponents (Brusco, 1982; Piore & Sabel; Rasiah, 1994; Sengenberger, Loveman, & Piore, 1990; Wilkinson, 2013).

Institutional change in the face of cyber threats has set into motion the changes of organisational practices in the critical sectors in becoming more risk averse. A neo-institutional theory has also been central in explaining organisational change where organisations tend to become similar with others in its population, hereby referred as isomorphism, a work by DiMaggio and Powell (1983). DiMaggio and Powell (1983), contends that decision-making for organisational change can be influenced by three mechanisms namely, coercive, mimetic, and normative. Coercive refers to pressure resulted from legislative related factors, such as mandate by the government to adopt certain practices in organisations. Mimetic explains how organisations tend to model themselves after others in similar field when they observe uncertainties in their environment. An example is when organisations are pressured to imitate others due to benefits gained from effective information security risks management (Steinbart et al., 2012). As for normative, it was derived from professionalisation. When groups of employees go through professionalisation process, formal educational standards and relevant certification are necessary. This is important when they need to perform tasks in a similar field for easier interactions as they observe issues in the same manner (DiMaggio & Powell, 1983).

The role of institutions is obvious in setting cyber security landscape for many countries. For most states in the United States (US), their Internal Revenue Service requires security incidents to be notified to them within 24 hours (Deloitte, 2014). Requirements set by the Federal Information Security Management Act in the US asserted the needs for security assessment to be conducted periodically in organisations to identify areas for improvement (Mohammed, Mariani, & Mohammed, 2015).

2.2.6 Power Distance

Previous cross-cultural studies have adopted a study by Hofstede (1980), that provides understanding on the effects of cultural aspects in organisational behaviour. There are four dimensions derived from a study based on 40 countries; collectivism versus individualism, power distance, uncertainty avoidance and masculinity versus femininity (Hofstede, 1980, 1983). The domain that is relevant to be adopted in this study is power distance. Power distance is the degree of inequality where the fundamental concern in this dimension is how inequalities in power are distributed and dealt with in a society (Hofstede, 1980, 1983). It also refers to the extent to which the less powerful group accept power that is distributed unequally.

According to Hofstede (1980), in a hierarchical culture with high power distance; those who are younger and low ranking are obliged to respect and submit to those who are older and with higher ranking. Countries that have high power distance prefer centralisation in decision-making in organisations where lower level employees are naturally comfortable to rely upon higher level persons (Sweetman, 2012). This can create a positive effect in organisations. A study conducted by Pasa (2000) in Turkey demonstrated that a leader granted with power or authority could influence compliance in organisations. Turkey was ranked by Hofstede (1980) as one of those countries that had high power distance value dimension where the citizens could accept power inequality in their organisations and institutions.

2.3 Empirical Works

This section reviews the cyber security landscape, peoples' behaviour in handling information security, information security awareness, communication of information security in organisations, cyber security compliance, top management commitment, security investment, structured security processes, technical information sharing and the governance of cyber security.

2.3.1 Cyber Security Landscape

The past decade saw the evolution of the motives for cyber security attacks and how innovation has influenced our way of living where mobile devices, smart phones, cloud computing and social networks have dominated the ecosystem. We have also seen how cyberattacks were not only carried out by individuals or group of individuals, but also by nation states that carried out their own agenda. In the year 2010, Stuxnet was designed to attack Iran's uranium enrichment plant. This incident opened many eyes on how sophisticated a cyberattack could be without even stepping on physical land (Langner, 2011; McConnell, Chertoff, & Lynn, 2012). But, that is not the only threat which nation states need to worry about. Cyber espionage is an impending threat to many developed and research-rich countries. Evidence by McConnell, Chertoff, and Lynn (2012) has shown that China has aggressively stolen proprietary technologies and intellectual property and converted them into fast and cheaper products. With the latest development and trend, the power of social media on the Internet should not be underestimated as it was capable of over-throwing the President of Tunisia, President Zine El Abidine Ben Ali, through people demonstration (Ghannam, 2011).

2.3.1.1 Cyber Security in Critical National Infrastructure

As deliberated in sub-section 1.7, critical national infrastructure in most nations comprises financial, healthcare, energy, water as part of sectors that are to be protected. In the event of cyber security incidents, the effects of failure in one sector can have cascading effects on other sectors. Specific sectors such as water, energy, transportation and gas use control systems which lack the necessary security features. When these systems are connected with corporate networks through the Internet, they create weaknesses that could be exploited by cyber perpetrators because they lack the necessary security features. Critical national infrastructure consists of complex systems and interconnected systems that is the backbone of many states. Although different jurisdictions have different approaches in protecting their critical infrastructures, they provide a common mechanism in protecting their national critical infrastructure that is through formulation of national policy and issuance of directives (Shamir b. Hashim, 2011, 2017; Warren & Leitch, 2011). The United States has identified eight (8) critical infrastructures, the United Kingdom identified eleven (11) and the European Commission also identifying eleven (11) sectors (Lukasik, 2011). Infrastructure has been defined by Hausken (2007) as assets that provide support in a country for its population's basic needs such as telecommunications, utilities, healthcare, transportation, financial, water and energy. In the absence of security features, the increase of interdependencies amongst these infrastructures would threaten these critical sectors and the public if attacks become successful. Therefore, protecting the critical infrastructure is the essential instrument in protecting the cyber commons (Lukasik, 2011).

2.3.1.2 Cyber Attacks in Critical Sectors

In September 2012, several big banks in the US such as JP Morgan, Citigroup, and Bank of America to name a few, experienced distributed denial of service (DDos) attack. This attack overwhelmed the banks' websites with traffic from computers that have been hijacked by cyber attackers. Not only did they attack the websites, to make the situation worse, the attackers also took control of commercial servers that have caused bandwidth congestion and left services unavailable to online clients (Strohm & Engleman, 2012). There were speculations as to who the attackers were. A group named Izz ad-Din al-Quassam Cyber Fighters claimed that they did it for a revenge attack as they felt offended being Muslims when Prophet Muhammad's video was uploaded (Strohm & Engleman, 2012). However, it was also believed that that these DDos attacks could have been due to revenge by Iran over the Stuxnet attack on its Natanz nuclear facility (Vaas, 2012). Although the financial industry is well- known for having huge budget allocations for Internet security controls and better governance compared to other industries, the DDoS incident in this sector in the USA have raised questions that if the financial industry which has extensive defence could not handle these attacks, what about the other critical sectors?

2.3.1.3 Cyber Attacks in Government Sectors

In recent years, the Government sector have been the target of attackers where top secret and sensitive information have been disclosed online due to stolen data and information; consequently affecting national security. The leak of sensitive information by Snowden has raised concerns on the trust that we have placed on contractors, third parties or even one's own employees in maintaining confidentiality (Starr & Yan, 2013). Not only data was stolen from the government sector, but identities of credit card holders or online banking consumers have also been a target for underground black market business where the breached data was worth at the average of US$200 per record (Williamson, 2014). Stolen data not only occurs in the financial sector but also in other sectors including universities. Most cyber security breaches that occur in universities were due to stolen credentials used by attackers to explore the target's systems network (Dearden, 2015; Stevenson, 2015). In 2012, a group of hackers by the name Team GhostShell hacked 53 universities in the US including elite and top universities and published the students' personal records to 'pastebin' website, a website where hackers normally dump stolen information online (2012). However, GhostShell was not financially motivated, but was a response to dissatisfaction to changes in the education law and increase in tuition fees. In another incident in the University of Birmingham, the motive for attack was personal when a student changed his grade after he managed to access the system and stole the staff credentials (Dearden, 2015).

2.3.1.4 Attacks on Control Systems

Supervisory Control and Data Acquisition (SCADA) is one of the critical components in the control systems that are connected with ICT systems. These components are proprietary systems designed for performance without security features (Igure, Laughter, & Williams, 2006). Prioritization of these systems are also different as power automation systems' priority is to ensure availability for the public use while ICT systems are prioritized to ensure confidentiality (Line, 2013), integrity and availability.

The Stuxnet worm that attacked the Iranian nuclear facility in 2010 has also been cited as the most sophisticated attack ever. Security analysts have also dubbed Stuxnet as the first cyber weapon targeting control systems (Farwell & Rohozinski, 2011; Nicholson et al., 2012). Stuxnet has caused damage to the Iran's nuclear programme that has also caused spill-over effect to other countries including India, Indonesia, China, Azerbaijan, South Korea, Malaysia, and the United States to name a few (Farwell & Rohozinski, 2011). Cyber security breaches have also been observed on other users of control systems like the Saudi Arabian national energy company - Saudi Aramco and Qatar's RasGas giving the indication that potential threat of cyber attacks in the oil and gas industries is imminent (Boman, 2012).

2.3.2 People Behaviour

Previous literature has suggested that the 'people aspect' has been widely regarded as the weakest link in organisations pertaining to information security (Bresz, 2004; Sasse, Brostoff, & Weirich, 2001; Vroom & Von Solms, 2004). Due to this situation where the digital commons or the Internet is an open system where members can come and go at their own pace (Pfeiffer & Nowak, 2006), the common goods produced on this platform are prone to exploitation by users whether they are internal (employees) or external (hackers); thus making it impossible to control.

Previous studies have also suggested that one of the effective approaches in mitigating cyber security risks in organisations is by getting employees to comply with security policies and procedures (Cheng et al., 2013; Ifinedo, 2014). However, there has been limited studies that associate human behaviour with information security compliance in Malaysia. A number of works related to cyber security were produced since the inception of the Internet in Malaysia (Muniandy & Muniandy, 2012; Shamir b. Hashim, 2011, 2017; Sonny Zulhuda, 2011, 2012; Zahri Yunos et al., 2010). While the major contributions of these studies are related to policy and cyber security in general, very few studies have really explored users' behaviour in association with information security compliance. The closest works related to this domain is by Safa, Von Solms, and Furnell (2016) and Noor Ismawati Jaafar and Adnan Ajis (2013). However, their studies did not capture human factor that constitutes user's behaviour in complying with security requirements. It is worth noted that humans have also been regarded as vulnerabilities to organisations where they can be easily exploited (Kraemer, Carayon, & Clem, 2009).

2.3.3 Information Security Awareness

Information security awareness programmes involve education and training (Parsons et al.; Siponen, 2000). Siponen (2000), posited that awareness programmes are able to motivate users to adhere to security requirements and further suggested that awareness should naturally be prescriptive in nature. This is to ensure that when users participate, they will not only learn to protect information in their systems but also avoid becoming victims of social engineering attacks.

Using the theory of Planned Behaviour (TPB), Safa et al. (2015) demonstrated that awareness programmes are able to change users' attitudes towards information security through learning stemmed from the programmes. This is supported by Bulgurcu, Cavusoglu, and Benbasat (2010) that information security awareness influences the attitude of end-users in complying with information security policies through rational theory. Ifinedo (2014), has also demonstrated that users' participation and social bonds created through awareness sessions are able to influence users in complying with security policies and procedures.

2.3.4 Communications

Communications are paramount to induce employees' behaviour to act responsibly in dealing with information on the Internet; thus making them cooperate in responding to security plans and measures initiated by the organisations. In an experiment conducted by Jerdee and Rosen (1974), communication plays a significant role in creating socially responsible norms for group members to produce behaviour that benefits those with the common interest. This study exhibits the significance of having members in groups to provide commitments for them "to act in a socially responsible manner as a means of producing behaviour in the common interest" (Jerdee & Rosen, 1974, p.716). In the context of information security, for information security efforts to be effective, users should be well-informed on what actions they should take (Adams & Sasse, 1999; Albrechtsen, 2007). Policies and procedures should be well-communicated to employees, so they know what needs to be done pertaining to security implementation in organisations (Von Solms, Rossouw & Von Solms, Basie, 2004). Employees should also be reminded on the availability and existence of security documentations such as manual, standard operating procedures, and other related materials and on how to access them (Puhakainen & Siponen, 2010).

A lack of communication (Adams & Sasse, 1999; Reich & Benbasat, 2000) can also decrease responsiveness (Teo & Ang, 1999) in the event of security events occurring. Further, it does not optimise the abilities of security teams (Ahmad, Hadgkiss, &

Ruighaver, 2012). Puhakainen and Siponen (2010), concluded in their study that when all levels in organisations actively communicate on information security matters, it will motivate the employees in complying in a consensual manner. In addition, integrating security matters with other communication channels provides better platforms in ensuring the message is relayed effectively.

2.3.5 Security Role

Wylder (2003), was of the view that top management visibility is not significant in influencing employees' attitude in providing commitment for security compliance; instead, everyone should be responsible and accountable in complying with security policy. However, Puhakainen and Siponen (2010) showed that their findings contradicted with Wylder's (2003) view. Apart from end-users, there are other groups in organisations that are responsible for security in organisations namely, top management (Hu et al., 2012; Jacqueline, Shahram, & Thomas, 2011; Knapp et al., 2006; Kritzinger & Von Solms, 2005), middle management (Kritzinger & Smith, 2008) and technical operations (Furnell et al., 2009; Kritzinger & Smith, 2008). These groups have defined roles and responsibilities to ensure the objectives of protecting information are aligned with organisational goals and objectives.

The importance of information security in organisations demands top management commitment in ensuring that information security is managed with due care (Hu et al., 2012; Knapp et al., 2006; Wylder, 2003). Top management commitment in cyber security has evolved with time as sophistication of cyberattacks has increased. In previous years where organisations were not ICT dependent, a study conducted by Straub Jr (1990) indicated that there was less commitment demonstrated by management to information security including little budget allocation, unclear security benefits and little knowledge on security controls deployment. However, the latest statistics showed that 70% and 79%

of top executives in United States and United Kingdom respectively concur that involvement of board level and top management respectively are critical to ensure data breach is effectively attended to in organisations (Ponemon Institute, 2015). But, nowadays, organisations have emphasized the utmost importance of security for sustainability of their organisations. Kritzinger and Von Solms (2005), posited that top management is responsible for information security in organisations and directors are liable for business continuity. This is supported by a study conducted by Ponemon Institute (2015) that demonstrate the criticality of top management involvement in cyber security related matters is as critical as putting cyber security on a board agenda.

Middle management is viewed as those who influence strategic decisions to be made in organisations (Floyd & Wooldridge, 1992, 1994). This group consists of mainly Heads of Departments or sections who produce policies, procedures and guidelines that are expected to be implemented in organisations (Kritzinger & Smith, 2008). Kritzinger and Smith (2008), further posited that the technical management mainly oversees the technical security issues focusing on technical-oriented tools, knowledge and practices that are required in securing systems and protecting information. According to D'Onza, Lamboglia, and Verona (2015), a lack of technical competence among the top management requires technical specialists to support them in understanding risks related to Information Technology (IT) and assisting them to mitigate the risks accordingly.

2.3.6 Cyber Security Compliance

Compliance was identified as a significant key performance indicator in measuring organisational performance through documentation compliance (Khalifa & Khalid, 2015) and compliance to quality standards (Antier et al., 2014). Compliance was also a significant factor in measuring performance of corporate governance for easier decision-making by investors (Kocmanova & Simberova, 2012) and high quality water in Portugal as regulated by the World Health Organization (WHO) (Vieira, 2005). In this thesis, cyber security compliance achievement is used as the indicator in measuring organisational security performance for CNII organisations.

Previous studies deliberated information security compliance mainly from the behavioural aspects of employees in organisations. Thus, several theories were applied in these studies. Although these studies did not mention cyber security compliance specifically, their scope suggested information that is transmitted across the Internet. For those organisations that fail to comply with regulations within their sectors, implications are not limited to trust and reputation only but also in monetary form. For example, in the US, Health Insurance Portability and Accountability Act of 1996 (HIPAA) is strictly enforced in protecting the privacy of medical records in the healthcare sector.

2.3.6.1 Information Security Compliance and Associated Theories

Previous security researchers cited a strong association between security awareness programmes and information security compliance (Bresz, 2004; Puhakainen & Siponen, 2010; Safa et al., 2015; Straub & Welke, 1998; Vroom & Von Solms, 2004). Vance, Siponen, and Pahnila (2012), posited that users' habit towards compliance play a role in influencing the feeling of being threatened if they did not comply. By exposing the users to the benefits and costs of compliance, it may act as a factor that can influence them to comply (Bulgurcu, Cavusoglu, & Benbasat, 2010). Previous security compliance models also dealt with moulding employees behaviour through security policies, organisational and top management commitment (Bulgurcu, Cavusoglu, & Benbasat, 2010; Goo, Yim, & Kim, 2014; Kwon & Johnson, 2011; Safa, Von Solms, & Furnell, 2016). These studies associated several social theories related to security compliance behaviours in organisations. General deterrence theory associates fearlessness of prosecution for compliance to happen (Lee et al.; Straub Jr & Nance, 1990). This was supported by Janis

(1967) that a certain level of fear should exist in human beings for intended messages to take effect. While deployment of preventive and deterrent measures reduced computer abuse by employees (Straub Jr, 1990), protection motivation theory deals with three delinquent elements, i.e., motivation to avoid unwanted behaviour, severity of threat and vulnerability of threat (Vance, Siponen, & Pahnila, 2012). Johnston and Warkentin (2010), suggested that the threat factor can orientate users to adhere to security practices in organisations.

Rational theory posits that humans will act on the basis of rational decisions in relation to the utility of their action against the benefits arising from it, and risk of getting caught alongside the punishment meted to such crime (see also, Becker, 1968). It has been used to show how users attitudes and habits and their normative beliefs are shaped by rational conduct in complying with security policy (Bulgurcu, Cavusoglu, & Benbasat, 2010; Pahnila, Siponen, & Mahmood, 2007). Ajzen (1991), advanced the theory of planned behaviour, which was subsequently appropriated by Ifinedo (2014) and Safa et al. (2015) to demonstrate the three components of attitude, subjective norms, and perceived behavioural control to shape individual behaviour towards information security compliance. This theory emphasizes the behavioural intention of an individual to perform such a given behaviour that they need to comply with. Safa et al. (2015), went further to discuss how attitude towards a certain behaviour can be modified through changes in the evaluation of factors, such as issues and events by learning either through awareness or training.

The social bond theory (Cheng et al., 2013; Safa, Von Solms, & Furnell, 2016) suggested that bonds created socially among employees are capable of minimizing antisocial behaviour that could deviate employees from complying with security policies and procedures. Another approach to security compliance is to understand the information security climate in an organisation where apart from security policies and awareness programmes, top management are significant for the compliance (Goo, Yim, & Kim, 2014).

2.3.6.2 Issues of Compliance

To some organisations that experienced security data breaches, being compliant by meeting requirements in the compliance checklist does not guarantee that their systems and information are secure (Valentine, 2010). Non-compliance with regulatory requirement can implicate not only the reputation and revenue of organisations but can also penalise to those who do not comply to the regulations (Basu, 2014). In an incident where an insurance company Zurich UK failed to take reasonable care by ensuring measures were taken to protect their customer data, the company was fined £2.275 million by Information Commissioner's Office in the UK, the largest fine at that time for data security failure (Condon, 2010). However, being compliant with regulatory requirements does not indicate good health of the security posture of any organisation (Basu, 2014; Mohammed, Mariani, & Mohammed, 2015).

Meanwhile, Valentine (2010) argued that when organisations are being too complacent with their compliant status coupled with a lacking of monitoring, this situation can potentially create security breaches to occur. His argument was based on the scenario where organisations in the US had to comply with Payment Card Industry Data Security (PCI-DSS) standards. PCI DSS is a proprietary information security standard for organizations that handle prominent credit cards such as Visa, MasterCard and American Express. Valentine (2010), further asserted that organisations have the mindset where upon complying with this standard, these organisations feel secure and will not experience future security breaches. Even the CEO of Target Corporation discovered that his organisation was being compliant even before the security breaches occurred in his organisation (Basu, 2014). What has been overlooked is that although the payment related systems are compliant, other aspects or controls connected to these systems as part of the environment tend to be ignored or less emphasized in terms of their security features.

2.3.7 Top Management Commitment

In ensuring that security requirements are complied with, it has to be based on top down approach. Commitment demonstrated by the top management to actively participate in information security programmes can motivate employees to comply with security requirements. For example, signing the security policy by the CEO demonstrates the top management's commitment in information security aspects in organisation (Von Solms, Basie & Von Solms, Rossouw, 2004). Puhakainen and Siponen (2010), in their study observed that management that were reluctant to follow security instructions, gave a signal to the employees that they were not committed in implementing security efforts and thus, demotivated the employees to comply.

In a study conducted by Cooper (2006) on employees' behaviour towards safety performance, one of the findings showed that visible continuous behavioural support showed by the top management was positive in exerting employee safety behaviour at the workplace. In addition, the frequency of interactions between management and employees indeed demonstrate a positive association in influencing the safety performance. It is also important to note that the degree of influence varies at different levels of management ; where top management has the most influence on an employees' behaviour compared to middle and front-line managers (Cooper, 2006). The involvement of top management through their commitment and support determine the success or failure of projects in organisations (Azizan Ramli, Mazlin Mokhtar, & Badhrulhisham Abdul Aziz, 2014; Chan Wai Kuen, Suhaiza Zailani, & Yudi Fernando, 2009). The commitment provided by the top management is not only in the form of behavioural and moral aspect, but also in terms of budget and resources allocation (Azizan Ramli, Mazlin Mokhtar, & Badhrulhisham Abdul Aziz, 2014). Similarly, top management commitment can also determine the overall effectiveness of security in organisations (Hawkey, Muldner, & Beznosov, 2008). Proviti (2016), posits that one of success factors in establishing cyber security measures effectively in organisations is through active engagement of board members in organisational information security risks.

2.3.8 Security Investment

The decision for organisations to invest in security is mainly motivated by two things; when required rate of return is higher than cost of attacks or when formal requirements are mandatory. Hausken (2006), posits that organisations which invested in security did so mainly due to regulatory requirements in complying with formal controls such as the US Sarbanes-Oxley Act of 2002 (SOX). The increase of ICT and Internet dependencies demands organisations to synergise security with its core businesses that could leverage security as added advantage to their business. This is where cyber security capabilities is embedded deeply within operations in organisations. Such deep embeddedness is not only to enhance business prospect but also to gain stakeholders' confidence in the organisations. Frequently, information security scholars refer to three fundamental factors in information security that need to be prudently managed; people, process and technology (ISACA, 2011; Posthumus & Von Solms, 2004, p. 639; Veiga & Eloff, 2007, p.38).

2.3.8.1 Security Technologies Investment

Organisations invest in security mainly to improve the security of its network and perimeter. Although deployment security technologies do not guarantee a secure ICT environment in organisations, it helps in preventing an organisation from being attacked and thus, minimizing its impacts. Surprisingly, some statistics show that there is a reduction of the deployment of these tools (CSI, 2010, p. 35; PricewaterhouseCoopers, 2012, p.16). Based on the Verizon study (as cited in CSI, 2010, p.35), organisations are overwhelmed with the quantity of data from the network monitoring logs that they fail to see the early signals produced by the system. However, these security tools are not independent. This means that they require either human or automated features in making themselves useful and effective in place.

Assuming that all technical measures such as anti-virus, intrusion detection system (IDS), firewall are sufficient in protecting information transmitted across the network, it can still give a wrong signal to organisations (Dey, 2007). Verizon (2013), reported that only 1 % and 3 % security breaches events were discovered from intrusion detection systems and log review process respectively. These low percentages of detection raised questions to system users whether deployment of these tools have been effective in detecting potential security breaches. This could be explained on the need to have technical capabilities in deployment of technical security controls (Ben-Asher & Gonzalez, 2015; Von Solms, 1997). However, a report by Verizon (2013), suggested that end users are still the most effective means in detecting security breaches.

2.3.8.2 People Investment

Besnard and Arief (2004), looked at successful attacks that lead to cyber security breaches as a combination of weak protection and malicious intents. Due to high dependency on ICT by many organisations from the industry and from the government sectors, they need people that possess not only ICT security technical skills and competencies, but also those with relevant management skills. The needs of these skills and competencies are becoming increasingly critical with the fast changes of the technology and recent development of the cyber security breaches and attacks and threats. Organisations invested in security technologies and expertise to build capabilities in detecting and containing data breach, where the longer breaches left undetected, the higher the cost to recover them (Ponemon Institute, 2016). This can be challenging to organisations in carving incentives in order to motivate them and retain their skills and capabilities within the organisation. Due to insufficient skilled and competent staff in cyber security, outsourcing related functions has been identified as one of the solutions in bridging the talent gaps (Deloitte, 2014).

Investing in security mechanisms in the context of security defence is not the only agenda in organisations or nation states, but many combine defensive with offensive modes. North Korea is one of the countries that have immensely blocked Internet access to cut their people off from the outside world lifestyle (Peterson, 2014). However, they strongly believe that cyber is the strongest weapon and thus, have made a huge investment not only to defend themselves but also to attack parties that do not seem to make them happy. In North Korea, through Bureau 121, a carefully selected team of 1,800 hackers, the country has made them sophisticated cyber armies who live in an elite lifestyle (Peterson, 2014). Despite their consistent denials, it is believed that Bureau 121 was behind the recent hack of Sony Pictures for not being sensitive prior to the release of the movie "The Interview" that implicated the country' s leadership lifestyle (Peterson, 2014). In a cyber war, attackers can focus on a single point of vulnerability to win the battle, but defenders need to work on all aspects of defending. Thus, budget is allocated not only for technology but also for the non-technology aspects in building capability for both defending and offending (Swarts, 2015).

2.3.8.3 Regulatory Pressure on Security Investment

Gartner reported that global total information security spending increased by 7.9% to A$71.1 in 2014 which was expected to be further increased by 8.2% in 2015 (Moore, 2014). The increase was due to regulatory pressure on the enactment of data and information protection in countries like China, Singapore and Malaysia. However, not all organisations can afford to spend on security, which explains the wide range of amount spent on security compliance that is between 1 to 2 percent and 10-12 percent (Johnson & Goetz, 2007). Upon the increase of governance requirements on information security, organisations have invested in people and technologies as means to defend themselves from cyber security attacks. Results of the survey conducted by the Council of Competitiveness (as cited in Damianides, 2005, p. 77) shows that that security investment has been regarded as good investment where 71 percent of respondents said that upgrading security in their organisation gave positive returns to their organisations. In contrary, Jerman-Blažič (2008) argued that most organisations still consider that spending on information security as expenditure instead of investment. This could be due to lack of ideal model to be adopted by organisation in making such investment. However, Jerman-Blažič (2008) later propounds the view that investing in security technologies is a security strategy in minimizing security risks and threats.

Frequently, as organisations were pressured in complying with regulatory requirements, the level of investments needed will increase in order to avoid security being breached (Cavusoglu et al., 2015). However, not all organisations have the luxury to invest in information security tools or the latest security technology due to financial constraints. Even if they have it, the budget has been shrinking (PricewaterhouseCoopers, 2012, p. 13). In a study conducted in the US, although half of the respondents declared a budget increase on cyber security initiatives in their organisations, some of them cited that lack of funding was one of the challenges in addressing cyber security issues (Deloitte, 2014).

2.3.9 Structured Security Processes

In information security, tasks associated with protecting information requires interdependencies and involvement of employees in two security processes; proactive and reactive processes. In ensuring information relevant to organisations or businesses are secure when it goes across the network, its confidentiality, integrity and availability need to be protected (Posthumus & Von Solms, 2004) which can be achieved when these security processes are in place. Key processes such as risk management has been identified as a critical component in information security (Schneier, 2000; Suhazimah Dzazali, Ainin Sulaiman, & Ali Hussein Zolait, 2009) and is also one of the measurement indicators in information security study (Suhazimah Dzazali, Ainin Sulaiman, & Ali Hussein Zolait, 2009). Other key security processes include business continuity management and incident management plan which are also capable of reducing cost of data breach (Ponemon Institute, 2016).

2.3.9.1 Proactive Security Processes

Proactive processes are processes that are designed and prepared by incorporating relevant tasks in order to mitigate information security threats, so actions can be taken before any event occurs. Three main processes discussed in this thesis are risk assessment, business continuity management and security vulnerabilities assessment.

One approach to managing information security is through the implementation of Information Security Management Standard (ISMS), a risk-based approach which is based on ISO/IEC 27001. ISMS has demonstrated the capabilities of an organisation in reducing risks and threats of information assets in organisations (Dey, 2007). To complement the technological perspective of security management, risk management has been identified as a mechanism to manage information security (Suhazimah Dzazali & Ali Hussein Zolait, 2012).

Although risk assessment should be conducted periodically, organisations tend to overlook the need to assess risks associated with a simple implementation process such as allowing mobile access to corporate network. Through this exercise, security strategy can be identified to mitigate the exposure of an event. PricewaterhouseCoopers (2012, p. 16) posited that security strategy deployed to address personal devices in workplace has not been sufficiently addressed in organisations where only 45 percent of respondents indicated that they have the strategy in place despite the high number of adoption of personal device for work (for example, bringing their own telephones to access corporate emails) and personal purposes (for example, bringing the same telephones to check their personal interests) which is at 88 percent of the respondents. ISMS provides the necessary information security governance framework that allows organisations to create provisions for human behaviours through initiatives with the objective of embedding information security culture in organisations (Veiga & Eloff, 2007).

Previous security scholars suggest that security vulnerabilities or weaknesses in software contribute to cyber security breaches (Anderson, 2001; Anderson & Moore, 2006; Schneier, 2007). Software becomes insecure when it is designed poorly with a lack of security testing (Schneier, 2007). Without proper security testing, security vulnerabilities will not be able to be identified; thus, they could be exploited when they were not properly patched (updated). Many organisations have been proactive in protecting its networking environment by performing security posture assessment that include assessing vulnerabilities on its networks, servers as well as the website and penetration testing to check the strength of the network against perpetrators.

Vulnerability assessment and penetration testing can be both performed as an annual exercise or when a new component of network or new system is being deployed that can become insecure due to disfigured systems (McElligott, 2006; Permann & Rohde, 2005). Security assessments are normally performed by external parties which means additional cost to organisations. It can be a challenge to organisations in providing budget justification. Although it does not give a pure return on investment of doing the assessment (Permann & Rohde, 2005), it helps to assess risks and understand where the biggest risk in the system is (McElligott, 2006; Permann & Rohde, 2005). One of crucial security processes in ensuring availability of information for organisations to use is Business continuity management (BCM). Its structured processes allow organisations to plan, recover from security breaches and continue operations with minimal impact. Embedding continuity practices in organisations through business continuity management helps organisations to stay alert and be prepared in the event of IT security breaches (Järveläinen, 2013) through continuous cooperation, support and teamwork from all business units within the organisation (Aronis & Stratopoulos, 2016).

2.3.9.2 Reactive Process

Reactive processes include those processes that are designed in reacting to security failures in organisations. A very important reactive process is responding to incidents and analysing data about incidents after the event (International Organization for Standardization, 2011). Cyber security professionals and practitioners agree that having the capabilities in handling cyber security incident is the foundation in minimizing adverse effects that cyber security incidents have on organisations. The root cause of security incidents need to be identified immediately after the incident for remedial actions (Mohammed, Mariani, & Mohammed, 2015). An established Computer Emergency Response Team (CERT) with proven incident management procedure is not only capable of containing the incident situation but is also able to identify and provide improvement upon gathering and analysing digital evidence on the compromised devices.

In Malaysia, establishing the CERT team in CNII organisations as one of the guiding principles of its National Cyber Crisis Management framework signifies the importance of managing the incident before it becomes a crisis not only to the organisation but also to the country (National Security Council, 2012).

2.3.10 Technical Information Sharing

It has been identified that the key to improve cyber security in organisations is sharing information relating to cyber security aspects including vulnerabilities and threats especially sharing defence data. Studies have provided evidence on the economic benefits of information sharing. A study conducted by Gal-Or and Ghose (2004) has demonstrated that information sharing has created two major effects; market expansion by increasing demands and also reducing price competition thus, eventually making higher profits. Gal-Or and Ghose (2004), further added that information sharing provides more benefits to bigger organisations and industries based on how they appreciate such information. Through a game-based modelling, the study also showed that an increased investment of security enhanced technology by a firm was able to accelerate the level of information sharing by the other firm (Gal-Or & Ghose, 2004). However, lower demand in one firm reduced the investment in security enhanced technology; thus lowering the information sharing level. It is evident that when firms share information on security activities there will be less expenditure incurred by each firm compared to when information sharing is absent (Gordon, Loeb, & Lucyshyn, 2003). The sharing gradually achieves the same level of security amongst them with a smaller cost to each firm; thus increasing the total social welfare.

2.3.10.1 Benefits of Technical Information Sharing

Information on threats and vulnerabilities are commonly shared amongst the security organisations and relevant communities. Most nation states incorporate voluntary based approaches like cyber security related task groups such as CERT to provide assistance and support in handling incidents reported by organisations and the public (Langevin et al., 2008; Lukasik, 2011). Relevant threats and vulnerabilities information between these CERTs are shared and discussed which was later incorporated through their websites for the benefits of the Internet users.

Mohammed, Mariani, and Mohammed (2015), suggested that information on cyber security incidents should be shared within the healthcare sector in order to strengthen the overall incident responses amongst the organisations in the sector. Delay in identifying causes of an incident can delay in providing remedial actions amongst them. Gordon, Loeb, and Lucyshyn (2003), found that sharing information on security breaches is able to assist organisations in resolving security problems in addition to technical solutions deployed. However, there are challenges in sharing information between public and private sectors. Private sectors seldom share security threats and breaches experienced in their organisations mainly to avoid loss of customers and tarnishing their image by appearing to be insecure (CSI, 2010; Kjaerland, 2006). While in the public sector, information identified from classified resources and methods could not be shared to avoid exposure to risk on sources and methods used (Rosenzweig, 2012). Many organisations do not intend to share information on security incidents as they are afraid that the breaches would have negative impacts on their organisations. However, the advantage is that sharing this type of information is able to assist others in providing the necessary preventive measures to avoid similar attacks. Even, if organisations still experience it, the sharing of information on the remedies of the incident allow the affected organisations to recover sooner.

2.3.10.2 Information Sharing between Public and Private sectors

Information sharing between the public and private sectors with refined responsibilities has been discussed in literature and can be rather challenging (Gal-Or & Ghose, 2004; Rosenzweig, 2012). The private sector that mainly owns the critical sectors are responsible for managing and protecting their assets and ensuring they meet the public requirements; while the Government is responsible for the protection of national security (Langevin et al., 2008). To some extent, some new threats in the government sector could not be shared with the private sector due to classified information, whereas privacy issue prevents private sectors from sharing information with the government (Rosenzweig, 2012, p.11).

In protecting critical infrastructure assets in the US, their federal government has encouraged the establishment of Information Sharing & Analysis Centres (ISACs) to protect its critical sectors which are mainly owned and operated by private sector (Gal-Or & Ghose, 2004). ISACs are established based on sectors where only members within the sectors benefits from this establishment. However, this centralised coordinated centre initiated by the Presidential Decision Directive-63 was not fully implemented at the time of the study conducted by Gal-Or and Ghose (2004) due to a lack of incentive on information sharing. Recently, the U.S. Congress passed legislation on Cyber Security Information Sharing Act that provides protection from liability for companies that share cyber threat information voluntarily with the government and industry (2016). However, information shared under this Act is not limited to cyber security purposes only, but also applies to other crimes such as espionage and trade secret violations.

2.3.11 Governing Cyber Security

The role of governance as a tool in protecting the Internet and regulating cyber space to combat illegal activities has been widely discussed (Langevin et al., 2008; Lukasik, 2000; Lukasik, 2011). However, a lack of a centralised governance structure due to the nature of the Internet, makes it difficult to regulate behaviour of its actors. Cyber offenders can keep on attacking due to the difficulties in determining the origins of a cyberattack, thus leaving those offenders unpunished.

2.3.11.1 Cyber Security Governance

The growing dependence of organisations on ICT where information and data have significantly flowed over the Internet coupled with risks of being borderless have made cyber security governance a critical facet in any organisation. Scandals of information security have sent shockwaves that damaged confidence of stakeholders in many trusted organisations. The failure of Enron has stemmed the enactment of Sarbane Oxley Act (Gordon, 2002) where internal controls should be deployed and monitored. Although the issue has been very much associated with corporate governance, it has now spilled over to cyber security whereby required improvement on the corporate governance was also extended to cyber security.

Information security is not a mere technical issue; thus it should be addressed as a corporate governance responsibility (Musa, 2012; Posthumus & Von Solms, 2004; Von Solms & Von Solms, 2006; Williams, 2001). The board of directors that are responsible and accountable to the stakeholders of organisations should be informed of the state of security in the organisation as security objectives should be aligned with the overall organisational objectives. Security scholars have widely accepted that information security is part of corporate governance in organisations (Veiga & Eloff, 2007; Von Solms, Basie & Von Solms, Rossouw, 2004; Von Solms, 2005).

Information security governance is defined by the way information security related processes are directed and controlled not only within the organisation itself but between the organisation with stakeholders (Ashenden, 2008). IT Governance Institutes describes three main components in governing information security namely, leadership, structure of organisation and processes in securing information (Brotby, 2001, p. 12). Information security governance has been discussed in previous security literature where scholars posited that ISO 27001 or Control Objectives for Information and Related Technologies (COBIT) as two common tools in governing security in organisations (Dey, 2007; Von Solms, 2005). However, the former fits better for the purpose as the latter is mainly for governing IT where security aspects are very minimal. In many occasions, the responsibility of governing information security are often left to middle managers or technical managers (Williams, 2001). For information security to be prudently governed, it should be addressed at the top management level (Posthumus & Von Solms, 2004; Williams, 2001) who are able to influence the operational activities in putting sufficient resources to improve security performance in organisations.

Although cyber security governance models are limited, there are several information security models available to guide cyber security activities organisations (International Organization for Standardization, 2012; Posthumus & Von Solms, 2004; Von Solms & Von Solms, 2006; Williams, 2001). Most of these models suggested risk management, top management and board of director commitment, stakeholders and continuous monitoring and control as key components in governing information security.

2.3.11.2 Established Security Governance Structure and Senior Leadership

The governance of information security requires a formal organisational structure which provides clear authority that is able to facilitate and coordinate information security in organisation (Kayworth & Whitten, 2010; Von Solms, Basie & Von Solms, Rossouw, 2004). Security functions, roles and responsibilities, communication on information security need to be clearly defined for a smooth implementation of security policies and standards throughout the organisation (Von Solms, Basie & Von Solms, Rossouw, 2004). Having a senior management team member in driving information security initiatives in an organisation reflects commitment provided by the top management in establishing strong organizational values in embedding security culture in organisation (ISACA, 2011; Kayworth & Whitten, 2010).

2.3.11.3 Information Security Audit

Previous studies discussed the role of internal audit in organisations in providing independent review and analysis of information security (Kayworth & Whitten, 2010; Steinbart et al., 2012) and information technology (D'Onza, Lamboglia, & Verona, 2015) in organisations. Having a formal monitoring process in checking policy compliance is capable to create conscious behaviour among users for being detected when they do not comply to security policies (Beautement, Sasse, & Wonham, 2009). The increasing needs of IT audit is mainly due to regulatory pressure in improving IT governance; where top management expected more efforts in auditing policies related to information security (D'Onza, Lamboglia, & Verona, 2015; Steinbart et al., 2012). Similarly, information security implementation should also be audited to ensure organisations comply with their own security requirements.

2.3.11.4 Roles of Institutions

In cyber space, various players include individuals, organisations and institutions that use the Internet with diverse motives and objectives. However, the degree of their understanding in protecting information varies. Thus, roles of institutions embedded with enforcement element are hugely needed to secure and protect users. This clearly describes the capabilities of institutions not only in forming rules for societies and economies but also enforcing them in a formal or informal manner (North, 1991). Farrell and Knight (2003), deliberated on how institutional change can occur when those who are in a greater power position are capable of making changes. In a situation that involves the element of trust, the impact of this institutional change can be huge. When trust is lost between actors, this will eventually affect cooperation amongst them. In circumstances that are complex such as the existence of heterogeneity, institutions play mediating roles especially on non-linear relationship between group size and collective action (Poteete & Ostrom, 2004).

For traditional consumption goods such as fisheries or forests, over-consumption of these resources without controls can result in the goods being abused. The exploitation in the salmon industry in Chile signifies how the absence of enforcement in regulating the fisheries industry in the country resulted in long term adverse effects to sustain the industry (Iizuka & Katz, 2010).

Due to the economic characteristics of public goods that can be applied in cyber security, economics scholars have also associated the significant role of regulations and enforcement agents in resolving the cyber security issue (Anderson, 2001; Anderson & Moore, 2006; Lukasik, 2000; Lukasik, 2011). An interesting finding from CSI survey shows that organisations have doubts with the law enforcement in resolving cyber security incidents reported to them (CSI, 2010). This explains the drop in reporting the incidents from 35 percent in 2010 to 27.5 percent in 2009 where the public has lost trust and confidence in law enforcement. Based on a study conducted by PricewaterhouseCoopers (2016), in the United Kingdom, almost two-thirds of businesses have lost confidence in law enforcement in dealing with the increase of cybercrime that has seen its increase by 20 percent since 2014.

2.3.11.5 Liabilities in Cyber Security

For any cyber security breach that occurs, the liability does not only fall on the attackers, but also other relevant entities such as the organisation that hosts the equipment and devices, and the person-in-charge of the networks. Organisations need to implement security measures to prevent security breaches from occurring be it at the endpoint, gateway, network or other access. Organisations need to define sets and rules on who is responsible for the data, what type of data leave the network and computing device and how the data leave the network and computing device. There are three modes of data that need to be identified, monitored and protected by organisations which are data in motion (e.g., network data transit), data at rest (e.g., data storage), and data in use (e.g., endpoint actions).

After cyber attacks occur, there will be liability claims for the attacks. Nowadays, cyber attacks have become very sophisticated with various motives that not only involves individuals, but organised crime groups and nation states. There are several bases for liabilities. In certain situations, an attack that causes harm can be foreseeable. When Microsoft announced that one of its operating systems, “windows XP” was out of phase where supports were no longer provided, and that users should stop using it as they needed to find alternatives to keep on a computing system. Naturally, patches (security updates required to fix system weaknesses) and updates will be provided by the publisher (if using Windows operating system, then the publisher is Microsoft) to ensure bugs or vulnerabilities are taken care of, so as to prevent weaknesses of the operating system from being exploited by attackers. Thus, users are responsible to ensure they implement the security updates of the operating system they are using. Similarly, anti-virus software used by users need to be regularly updated by the latest signature to ensure the OS is protected against new malwares. Organisations need to also ensure that the person-in-charge of security of their computer systems are competent in providing security measures and controls to avoid the organisations from becoming liable due to unforeseeable attacks. For organisations that deploy systems which provide services for public consumption such as industrial control systems, due care must be in place to avoid cyberattacks that result in physical damages. In the US, failure to implement relevant security measures and controls in preventing foreseeable dangers is considered as being negligent where the negligence constitutes a breach of due care (that causes liabilities) to victims who are injured due to the incidents (Finch & Spiegel, 2014).

Typically in a cyber security breach incident, there are several entities; typically third parties such as security vendors (hardware or software) or Internet Service Providers (ISP) that are indirectly liable for the harm caused for example, a virus attack. Under strict liability, the ISP might need to monitor activities of their subscribers and identify hackers that could potentially spread the virus. As for the software security vendor, the vendor might need to incorporate all security measures required to minimize damage caused by hackers before selling it off to their customers. As for the organization whose own files were stolen by online perpetrators, the organisation could be strictly liable for the loss by taking necessary steps to protect their information from being stolen. Strict liability is also applied in a situation whereby activities engaged by a party is capable of providing more externalised benefits than cost to the related recipients (Hylton, 2007; Shavell, 1980). Shavell (1980), also cited the example of Internet service providers with operating system manufacturers that have jointly provided information as resources that benefit the Internet user. The virus creator who is responsible for the virus creation is unknown. In this situation, the application of strict liability to third parties like ISP and operating system vendors is inefficient as suggested by the public goods theory taking into consideration the external benefits gained by the Internet user associated with enhanced disseminated information (Hylton, 2007).

2.4 Summary

This chapter reviewed key theories and previous empirical works in developing the analytical framework to be used in answering the research questions. Although top management, security awareness and attitude have been identified as common factors in security compliance models, these models did not incorporate other organisational practices such as structured security processes, security investment and effective communications in their model to drive security compliance in organisations.

The review identifies several gaps which the study wishes to explore. Firstly; there were limited studies associating cooperative behaviour with cyber security compliance. This study seeks to explore social factors in organisations that influence users' intention to cooperate in achieving cyber security compliance. Even though there were empirical studies related to public goods, but there was none in the information security discipline that relates it to cooperation in organisations. Thus, this study applies the theory from a different approach. Using public goods theory as the foundation, the non-excludability characteristic triggers cooperative elements to be explored in understanding factors that constitutes cooperation.

Secondly, previous related studies discussed factors that only dealt with internal factors. These studies on security compliance mainly dealt with internal factors such as users belief, attitudes, rational beliefs and habits, fear of sanctions, the behavioural intention of an individual to perform to such a given behaviour, social bond creation and information security climate in organisation that influence users behaviour to comply with security requirements. Some of the models did not incorporate clear role of institutions in helping organisations to meet their compliance objectives.

Thirdly, there were limited studies that discussed the indirect effect of cooperation in explaining the relationship between organisational practices with cyber security compliance. Thus, this study wishes to analyse how cooperative behaviour among employees affects existing organisational practices in contributing to security compliance in the context of Malaysia environment. Previous studies demonstrated the direct association between various predictors with employee's behavioural intention to comply.

However, this study is to examine the mediation effects of cooperation have on these relationship.

Finally, there were limited studies that emphasized role played by relevant institutions that influence users to comply with security requirements in organisations. Previous studies related to information security compliance were limited to only one level that is at the organisational level. Thus, using the public good and institutional theories, this study wishes to investigate further the sector leads of the ten CNII sectors and central authority level, the National Security Council, as the institution responsible for governing cyber security in the CNII sectors in Malaysia.

CHAPTER 3: RESEARCH METHODOLOGY AND DATA

3.1 Introduction

The selection of a research method is crucial in setting the direction of a research project as it ensures that the data collected are valid and acceptable. In deploying an effective research technique, an in-depth examination of the research problem was accomplished in the previous chapter on literature review, Chapter 2, as it was fundamental to select the best technique to acquire data and analyse them. This chapter discusses the research methodology, strategies and justifications used to answer the research questions and fill-in the gaps that were identified earlier in Section 1.3. This chapter has six sections. Section two, begins with a high level discussion on the formulation of the research analytical framework. Section three discusses research mode and data followed by section four on the analytical method that covers the analytical techniques in answering each research question. This is followed by section five on pilot study before the chapter finally concludes in the summary section.

3.2 Analytical Framework

The analytical framework used in this study views that intention to cooperate leading to cooperative behaviour is the central factor that contributes to cyber security compliance. This study argues that cooperation plays a major role not only in organisational practices but also in governing cyber security in the CNII cyber security ecosystem. This study also argues that institutional roles have evolved from pure operational roles to embrace cyber security culture that could mitigate cyber security risks not only in organisations but in sectors and at national level.

The first research question of this study draws on the public good theory and cooperation to capture factors that influence employees to cooperate in complying with security requirements. The second research question focuses on how cooperation is mediated between organisational security practices and achieving cyber security compliance. The third research question focuses on the existing cyber security governance instruments at three levels; organisational, sectoral and national levels, and their efficacy in regulating cyber security compliance in CNII organisations.

The analytical framework to examine these factors and instruments and their relationship is shown in Figure 3.1. This figure illustrates factors that contribute to security compliance in organisations through the central subject of this study which is cooperation. The detailed use of the analytical framework and the variables are undertaken in analytical chapters 4, 5 and 6 respectively.

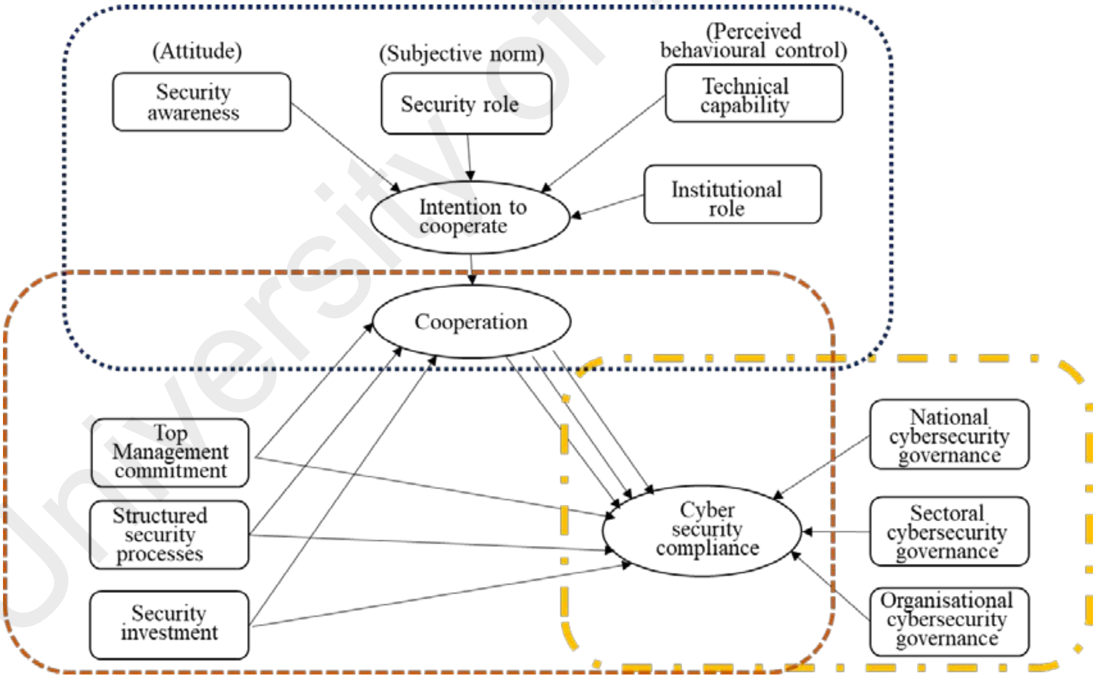

(Attitude)
(Subjective norm)
(Perceived behavioural control)
Security awareness
Security role
Technical capability
Institutional role
Intention to cooperate
Cooperation
Top Management commitment
Structured security processes
Security investment
Cyber security compliance
National cybersecurity governance
Sectoral cybersecurity governance
Organisational cybersecurity governance

Figure 3.1: Analytical Framework
Source: Author

3.3 Research Mode and Data

This study deployed both quantitative and qualitative approaches in answering the three research questions. However, not all research questions used the same approaches. In addressing research questions one and two, the data gathered from the survey instrument were sufficient in answering both research questions using the quantitative method. These items (in answering both research questions) are internal factors related to cyber security organisational practices that were explicitly stated in the instrument. Binary Logistic Regression (BLR) and Karlson-Holm-Breen method (KHB) were used in analysing research question one and two respectively. However, for research question three, the quantitative findings showed that the sectoral and national quantitative results were inadequate in answering the third research question. This was due to items in the survey instrument pertaining to sectoral and national levels that were general in context and subjective, which could open for interpretation. In addition to the national security documents provided by the central authority, certain sector leads issued their own directives or circulars. The rationale behind this is the needs for them to adhere with other security requirements specific to their sector and comply with international regulatory requirements. Therefore, in order to avoid inconclusive results in addressing the third research question, conducting interviews was necessary. It was also important to get an in-depth information of the deployment of these instruments at all levels to understand how they affected the cyber ecosystem in the country. Thus, a qualitative method was necessary to complement these findings in reaching a credible conclusion on the effectiveness of the instruments at the three different levels. For research question 3, the quantitative data was analysed using Ordinal Logistic Regression (OLR) method.

3.3.1 Quantitative Approach

For the quantitative approach the following sub-sections discuss the sampling method and respondents, the sample size, the survey instrument, data collection, data normality and reliability as in sub-sections 3.3.1.1, 3.3.1.2, 3.3.1.3, 3.3.1.4, 3.3.1.5 and 3.3.1.6 respectively.

3.3.1.1 Sampling Method and Respondents

This study applied purposive sampling. Although unbiasedness can be an issue in this type of sampling, Tongco (2007) argued that purposive sampling can be an effective tool and can be better than random sampling if deployed carefully. Allen (1971), posited that in deploying purposive sampling, it is crucial to source respondents who qualify as trusted informants in the study. Thus, the main criterion for choice of respondents is; information security background and knowledge. Because we were interested in understanding on how organisational practices mediated cooperation to achieve compliance, apart from significance of knowledge and experience in this domain (Rhee, Kim, & Ryu, 2009; Rocha Flores, Antonsen, & Ekstedt, 2014), our sampling also placed an emphasis on those who had critical roles in implementing security efforts in organisations. These critical roles were based on three groups, namely top management, middle management and technical management. The sampling procedure required voluntary participation from the organizations. Hence, all volunteers from the identified list of organizations were approached. This sampling was more practical where data was acquired from respondents with sound judgement based on qualities they possessed rather than random individuals in the organisations (Bernard, 2011).

For this study, respondents were selected from two databases; organisations from the ten (10) CNII sectors database and educational database. The ten (10) sectors that have been identified as CNII sectors, viz., Government, Defence and Security, Finance and Banking, Information and Communication, Energy, Food and Agriculture, Transportation, Emergency Services and Health Services. There are 200 organisations identified as CNII organisations (Shamir b. Hashim, 2017). For this study, education sector comprising of public and private universities were also included. Although universities are not directly listed under the CNII sectors, they are governed by the Ministry of Education. In terms of cyber security aspect, they are guided by the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), which is one of the sector leads[4] (National Security Council, 2012).

There are two levels of selection process for the respondents. The first level consists of selecting the participating organisations, and the second level consists of selecting respondents from the selected participating organisations. Participating organisations were subject to two criteria: first, CNII organisations identified by National Security Council were used. CNII organisations consist of public and private organisations as well as sector leads. Second, where a participating organisation was not a CNII organisation, it had to belonged to a CNII sector and be regulated by the respective sector lead. The derived sampling is depicted in Figure 3.2.

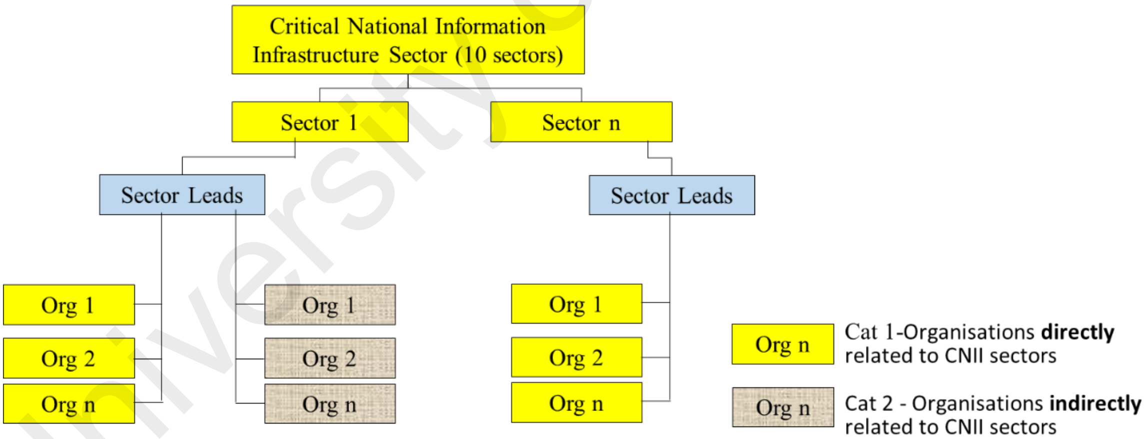

Critical National Information Infrastructure Sector (10 sectors)
Sector 1
Sector n
Sector Leads
Sector Leads
Org 1
Org 2
Org n
Org 1
Org 2
Org n
Org 1
Org 2
Org n
Org n
Cat 1-Organisations directly related to CNII sectors
Org n
Cat 2 - Organisations indirectly related to CNII sectors

Figure 3.2: Derived Purposive Sampling of Study
Source: Author

As for the second selection level, the main criteria for the respondents is that they should have an understanding and knowledge of information security in general and more specifically of the security situation in their organisations.

[4] Justification for including the education sector is justified in sub-section 1.4.

In order to capture responses that may vary using the similar survey instrument, criteria for respondents were further defined according to their level of security responsibility or their security role. The three groups that hold security responsibilities were namely, top management, middle management and technical management. The top management were those who set the organisational information security strategies and objectives and were accountable for any security breaches that might occur. They were those who hold the position of Chief Information Security Officer (CISO), Chief Information Officer (CIO), or similar who led the security team and efforts in their organisations. As from the middle management, this category were those who normally did the implementation as defined by their top management and ensure information security objectives were met. The third security group comprised those who dealt with the technical aspects of cyber security such as system administrators, network administrators or similar. These were the people who were responsible for ensuring technical security measures were in place and monitored network traffic for early detection of potential cyber threats. The significance of these different levels were that their responses could draw different conclusions based on the roles they played in their organisations.

This study also relies on assumptions that are reasonable but may not necessarily hold all the time. It is assumed that participating organisations have been served by the knowledge of their organisations being identified as organisations that are related to CNII sectors and relevant directives. For organisations that are not CNII agencies, they are assumed to have the knowledge on relevant directives furnished by institutions that regulate them directly or indirectly. It is also assumed that the participating organisations have the knowledge of security instruments that are extended to their organisations.

3.3.1.2 Sample size

In determining the sample size, this study used Yamane's (1967) sampling size formula (as cited in Israel, 1992, p. 4) as follows:

$$n = \frac{N}{N + 1(e)^2}$$

where N=population, e = level of precision

CNII sectors comprises 200 organisations (Shamir b. Hashim, 2017) whereby the educational sector comprises 66 universities (20 public and 46 private) (Kim Wai Lam et al., 2018). Based on the above formula, the minimum sample size needed to perform the analysis is approximately 160.

3.3.1.3 Survey Instrument for Quantitative Data

In this study, a survey instrument was developed for quantitative data collection purposes. Attached with the questionnaires was a letter explaining the objective of the study and assuring respondents' confidentiality of their responses. It is important to keep confidential both respondents details and responses due to the sensitivity of this study. The survey instrument is arranged into two parts. The first part consists of information on the demographic profile of the respondents. Respondent's characteristics such as security role, job portfolio, professional certification, employment service, tenure of service, sector they were in, and organisational workforce size were asked. The profile information is necessary as it influences the type of response given by the respondents.

For respondents' profile, eight items were specified: first, organisation type, second, workforce size, third, sector, fourth, security role, fifth, job portfolio, sixth, education, seventh, service tenure and eighth, professional certification. There were two types of organisations to be recorded; government related and private organisations. The workforce size reflects the population size of the respondents' organisation comprised of five groups; first, less than 100 employees, second, between 101 to 250 employees, third, between 251 to 500 employees, fourth, between 501 to 750 employees, and fifth, more than 750 employees. Sector has eleven categories, ten (10) critical sectors which have been identified as CNII sectors; 1) government, 2) national defence and security, 3) banking and finance, 4) information and communications, 5) energy, 6) transportation, 7) emergency services, 8) water 9) health services, and 10) food and agriculture and 11) education.

Security role has four categories to capture different levels of security role played by the respondents namely, top management, middle management, technical and other role (e.g. compliance and audit). Job portfolio has five categories namely, first, ICT security, second, ICT operations, third, ICT planning, fourth, risk management/compliance and fifth, other business units. These five categories were later collapsed into three categories for a better analysis. The first category comprised those who directly involved with ICT security and responsible to ensure the overall security was taken care of including systems, applications and physical. Next, groups were those who were indirectly related with security including ICT operations and ICT planning, ICT risks and other related tasks.

Tenure of service was measured by the length of time the respondents served the organisation. This variable is based on demographic data with four categories, first, less than 2 years, second, between 2 to 5 years, third, between 6 to 10 years and fourth, more than 10 years. Professional certification comprised certifications issued by global certification bodies and also product based certifications. This item was later coded as binary, 1 = have certification and 0 = no professional certification.

The second part comprises items on cyber security practices in organisations, types of security incidents and also their responses on the roles of their regulators as well as the central authorities. These items are discussed in subsequent chapters 4, 5 and 6.

This study chose a Likert scale to measure responses as it is suitable in assessing attitudes in social sciences studies (Bard & Barry, 2000; Spector, 1992). A survey using the Likert scale measurement allows respondents to provide answers that best suit their personal preferences and experiences related to the situation at that time. For this study, all variables are measured on a five-point Likert scale, ranging from (1= strongly disagree, 2= disagree, 3= neutral, 4= agree and 5= strongly agree).

In developing the questionnaire, six persons, of whom four were PhD holders in information security and two were qualified information security practitioners who were professionally certified, were consulted to obtain their feedbacks on the understanding and quality of the instruments and to identify areas for improvements. Copies of the instruments were presented to them and discussions were held as they went through the questionnaire.

In consulting them, improvements were made considering new issues that were brought up by them as follows:

1. Meaning: Whether the questions were understood and they had a similar understanding on the meaning.
2. Instructions: Whether instructions were clear in providing clarity for the respondents.
3. Questions difficulty: Whether the respondents could answer questions without confusion.

4. Willingness to answer questions: Whether the respondents were willing to answer because the questions were related to security practices that were sensitive in nature.

This study uses a combination of single and multiple items to establish predictive validity measures. The multiple-item scale or construct were later tested for their internal consistencies to ensure they are reliable for further analysis. Previous studies particularly in market research emphasized that better results were achieved using multiple-items to measure (Churchill, 1979). However, there were arguments on the level of acceptance of a single item measure. Using C-O-A-R-SE procedure, the stability of using single versus multiple items were further deliberated by Rossiter (2002) where a single item measure is acceptable if the object of construct is conceptualised as singular and concrete. Bergkvist and Rossiter (2007, p. 183), took it further and suggested that "theoretical tests and empirical findings would be unchanged if good single-item measures were substituted for these constructs in place of commonly used multiple-item measures". A single-item measure can produce high predictive validity in comparison to multiple-item measures if the earlier could be crafted carefully (Bergkvist & Rossiter, 2007, 2009). Although in most instances researchers were advised to employ multiple-item scale (Churchill, 1979), deploying single-item scale is still acceptable in certain circumstances (Diamantopoulos et al., 2012). Details of variables were discussed in respective analytical chapters.

There were 55 items in the instrument prior to the consultation stage. After three weeks, feedbacks were received where improvements were made for better understanding of the respondents where the items were finally reduced to 44. The questionnaire is as per Appendix A.

3.3.1.4 Quantitative Data Collection

Primary data collection was conducted in accordance with the criteria of respondents that have been discussed in sub-section 3.3.1.1. Data was collected through a survey period from 21 August 2013 until 31 July 2015. There are two methods of questionnaire distribution. The first method is that hardcopy questionnaires were distributed by hand to participants approached in cyber security related events such as cyber security conference, seminars, working group meetings and trainings. The data from these questionnaires were later manually entered into an online software “surveymonkey” (http://www.surveymonkey.com/). The second method is that upon identifying potential respondents that fit the criteria, requests for them to participate were made either through meeting them physically or over the phone. Upon their consent to participate, an official email would be sent together with the link of the software. A follow-up call would be made if there was no increase of observations on the online software. In this study, for the purpose of data collection, “surveymonkey” has been subscribed throughout the data collection period for respondents to enter their responses online and also for manual data entry.

3.3.1.5 Data Normality Analysis

It is important to perform data normality test to ensure a suitable analytical method is deployed in answering a research question. Common problems occurred when data values are too positively or negatively skewed. It is an important step to test its normality before proceeding to the main statistical analysis. Two types of normality tests were opted to test normality of the observations; Kolmogorov-Smirnov and Jarque-Bera statistical tests. One of the reasons to employ the latter was due to the nature of Likert-scale data collected from the survey instrument (Jarque & Bera, 1987; Thadewald & Büning, 2007). Therefore, we undertook normality tests using the Jarque-Bera goodness-of-fit test to see whether the sample data have the skewness and kurtosis that match a normal distribution

(Domański, 2010). For this test, the null hypothesis is considered as normal distribution for observations. To determine whether the null hypothesis is accepted or rejected, the test statistics of the variables were compared with critical values at 3 different significance levels; 0.1, 0.05 and 0.01. The null hypothesis cannot be rejected when the test statistic of a variable does not exceed the critical value at any of these three significant levels.

3.3.1.6 Reliability Analysis

The reliability test is concerned with the consistency and validity of the survey instrument. For this study, assessing internal consistency is opted to examine the level of inter-relation of items in groups of items in the questionnaire. Previous scholars (Gliem & Gliem, 2003; Nunnally, 1978) suggested that Cronbach's alpha internal consistency reliability value of 0.7 or higher is considered acceptable in research works. However, Suhr and Shay (2009), argued that 0.6 is acceptable if the analysis was for research purposes. Other researchers (Setbon & Raude, 2010; Waljee et al., 2010) have also accepted 0.6 in view of the claim made by Streiner and Norman (1989) that alpha value lower than 0.6 was insufficient while higher than 0.8 suggested items redundancy in measuring the construct.

3.3.2 Qualitative Approach

In answering research question 3, the qualitative approach was deployed mainly to complement the quantitative method (Pope & Mays, 1995) and to support quantitative findings that require clarification in concluding the study. The following sub-sections discuss the data sources and the instrument used to collect the data.

3.3.2.1 Qualitative Data Sources

Qualitative data of this study was drawn from various sources, such as interviews, document reviews, newspaper articles, and government documents. The government documents include laws, regulations, policies, directives, and historical resources. Apart from these government documents, interviewes were also conducted. Pope and Mays (1995), asserted that one of the qualitative techniques which was in-depth interviews used in this study could provide a clear understanding of a situation or behaviour that could clarify ambiguities found in the questionnaire (quantitative data).

For the interviews, open-ended questions were deployed to allow respondents to express themselves freely. Thus, the interviews were flexible enough because it was not possible to create themes out of the data collected. It is also not the purpose of the interview to categorise responses in themes. Instead its main purpose was to complement the quantitative data in filling the gaps from the quantitative analysis.

In order to understand the whole spectrum of cyber security in CNII sectors, organisations selected for the interview included the central agency, three sector leads, three CNII organisations and one public university. The list of interviews are listed in Table 3.1. The respondents for the interview were selected based on three criteria, namely, the criticality of the sector, their number and willingness to be interviewed. In other words, the interview was directed where there was a high number of respondents in the sector and where they had agreed to be interviewed and willing to participate in this study. Respondent selection was based on a set of criteria that took into account roles of respondents in their organisations and also willingness to participate. The latter criterion was crucial as to allow respondents to honestly provide the required information that could cause biasness in responses.

Table 3.1: List of Interviews

Name	**Organisation**	**Background of Respondent**	**Role of Organisation**	**Sector**
Respondent1	Organisation I	Information Security Expert for Security Compliance	Sector Lead	Government
Respondent2	Organisation II	Head of Information Technology Division	Sector Lead	Financial
Respondent3	Organisation III	Head of Information Technology Division	Sector Lead	Healthcare
Respondent4	Organisation IV	General Manager	CNII organisation	Information and Communication
Respondent5	Organisation V	Information Security Manager	CNII organisation	Information and Communication
Respondent6	Organisation VI	Head of ICT strategy	CNII organisation	Financial
Respondent7	Organisation VII	Information Technology Officer	Government organisation	Education
Respondent8	Organisation VIII	Principal Assistant Secretary on National Cyber Security Policy	The Central Authority	The Central Authority

Note: Interviews were conducted from September 2015 until June 2016
Source: Interviews conducted by the Author in 2016

Interviews were conducted face-to-face that took approximately one hour for each interview. In order for an effective interview to take place, a list of questionnaires were emailed to them prior to the interview.

3.3.2.2 Survey Instrument for Qualitative Data

For collecting the qualitative data, the questionnaires for selected organisations, sector leads and the central authority were designed separately from the quantitative method. The questionnaire is in Appendices B, C and D respectively. The separate list of questions were due to different questions asked for each group. There were several questions that were specific that attempted to gain insights into issues in terms of the overall processes among agencies, sector leads and agencies and the central authority. Most of the interviews lasted approximately an hour.

3.4 Analytical Methods

For the main statistical analysis, several regression analysis were conducted to examine the relationship between identified predictors and the outcome variable. Regression analysis was widely used in social and information security studies where relationship between predictors and outcome variables could be investigated (Gupta, Joshi, & Misra, 2010). Prior to performing analysis for all research questions, preliminary statistical analysis was conducted to identify suitable analytical method for each research question. The preliminary statistical analysis included descriptive statistics, normality test and reliability test. Normality test and reliability test were discussed in sub-sections 3.3.1.5 and 3.3.1.6.

Due to assumptions that were not met in terms of normality distribution of data for ordinary least squares (OLS), this study opted for BLR analysis in answering research question 1. As for research question 2, mediation analysis using KHB method was opted to test the mediation effects of predictors against the dependent variable. In answering the final research question, OLR was chosen in analysing the dependent variable that has more than two ordered categories. The details of these analytical methods are discussed in the next sub-sections.

Statistical Software Packages SPSS version 22.0 were chosen to perform preliminary stastistics, BLR and OLR whereby STATA Stata/SE 12.0 was chosen to perform the mediation analysis using the KHB method. Although SPSS software can perform mediation, the mediation function is limited to only continuous variable as for the dependent variable. Since the dependent variable in addressing research question 2 is categorical, STATA was opted to perform the mediation analysis.

3.4.1 Binary Logistic Regression

In answering research question one, this study deployed Binary Logistic Regression (BLR) analysis method. Compared to Ordinal Least Square (OLS) regression that uses a continuous dependent variable (DV) and linear in nature, Logistic Regression Models are appropriate when the DV is categorical (i.e., has two or more categories). For studies that have a dichotomous outcome variable, which have two values (e.g. zero or one), BLR is an appropriate option. BLR is widely used in information security studies (Bullée et al., 2015; Choi et al., 2008; Liu, Tanaka, & Matsuura, 2008). In BLR, the independent variables or predictors can be either continuous or categorical or a mix of both. BLR calculates the probability the success over the failure of an event, which is the DV. However, the prediction of the DV is not in terms of its value as in OLS, but a probability of continuous data of the DV between 0 and 1 (Burns & Burns, 2008). Thus, in order to best fitting the equation of this regression, BLR uses maximum likelihood method (MLM). In this method, BLR "maximizes the probability of classifying the observed data into the appropriate category given the regression coefficients" (Burns & Burns, 2008, p.569). Apart from predicting an event (e.g., pass or fail), BLT also analyses the relationships and the strength of the variables.

According to Burns and Burns (2008), assumptions to be met in performing this regression are as follows:

1. The regression should not have a linear association
2. The outcome variable must be a dichotomous variable
3. The independent variables do not need to be normally distributed or linearly distributed
4. The categories are mutually distributed where one case must be only in one group and one case must belonged in any of the groups
5. A larger sample is needed in comparison to OLS

However, a study by Peduzzi et al. (1996), suggested that the sample size needed for each case of DV is at least 10 cases.

This study uses the following to analyse the test of significance of the regression:

1. Log likelihood (LL) is used as the basis test for BLR. It is derived from the natural logarithm used in predicting the "likelihood" of the observed values of DV is predicted from the observed values of IVs (Burns & Burns, 2008).
2. Likelihood ratio test is used to test the significance of the difference between the likelihood ratio (LR) for the model with predictors minus the likelihood ratio for model with only constant in it (without predictors). It is based on -2LL ratio. If p value of the test is less than or equal to .05, then it shows that the model with predictors is significantly different from the one without predictors (Burns & Burns, 2008).
3. Model Goodness of Fit test method is used to test how well the data fits the model by assessing how close the observed and predicted events match. The null hypothesis suggests that "the model fits" will be rejected if the p-value is less than .05 (Burns & Burns, 2008). If the data fits well in the model, the observed and predicted events will be close, thus the test statistics value is small and significant.

3.4.1.1 Model Specification

As discussed earlier, due to the dependent variable is a binary variable, a logistic regression model is used for the statistical analysis purposes. In general, the logit model can be written as follows:

$$logit\ (p) = log\frac{p}{1-p} = \propto + \beta_i X_i + \varepsilon, i = 1, 2, 3, \ldots, k$$

where, p is the probability that an event will occur; $1 – p$ is the probability that an event will not occur; $p/ (1 – p)$ is the odds of the event to occur; X_i is the i^{th} independent variable that affects the probability of the event to occur; β are coefficients of the independent variables; and ε is the error term.

3.4.2 Karlson-Holm-Breen Method for Mediation

In answering the second research question, this study applied mediation test using the Karlson-Holm-Breen (KHB) method. KHB is a method used to perform statistical analysis for non-linear probability models, such as ordinal logistic regression model used in this study. Mediation was opted as it is an approach where a researcher could explain the association between one variable and another, through the intervention of the third variable (MacKinnon, Fairchild, & Fritz, 2007). Mediation is used by researchers mainly in studies related to psychology, social science and behavioural science in answering questions that require chain of questions and responses (MacKinnon, Fairchild, & Fritz, 2007). Baron and Kenny (1986) highlighted the S-O-R mediation model developed by Woodworth (cited in Baron & Kenny, 1986, p.1176) as the most generic mediation model where "the effects of stimuli on behaviour are mediated by various transformation processes internal to the organism". In other words, mediation describes how an independent variable (IV) affects a dependent variable (DV) through a variable that intervenes the relationship, thus affects the outcome.

Previous literature highlighted several common methods used in testing the indirect effects including causal steps (Baron & Kenny, 1986), the Sobel test (Sobel, 1982) and bootstrapped confidence intervals (Preacher & Hayes, 2008). Preacher and Hayes (2008), argued that the causal steps strategy is suitable for large samples, while the Sobel test has dependencies on the normality of data distribution, which also works well in large samples. Meanwhile, bootstrapping, which is a resampling procedure suits studies that do not impose the assumption of normality of sampling distribution (Preacher & Hayes, 2008).

For this study, the mediation effect of cooperation on the relationship between organisational practices and CSC was tested using the KHB method that uses non-linear probability models, such as ordinal logistic regression model (Breen, Karlson, & Holm, 2013; Pais, 2014). The KHB method was used as it resolves the problem of a rescaling of models that induced the joint identification of co-efficient and error variances, which frequently occurred in non-linear probability models. This statistical test decomposed the total effect into two types of effects, direct and indirect effects for non-linear models (Kohler, Karlson, & Holm, 2011). Contrary to linear models that were quite straight forward, scaling problems occurred in non-linear models as without mediating variables they frequently produced large standard error than models with mediating variables (Karlson & Holm, 2011). The KHB method rectified this problem through rescaling which enabled the comparison of the coefficients from both models (Karlson & Holm, 2011). The KHB method also compared the unadjusted model (total effect without mediator) with the adjusted model (direct effect with mediator) "by calculating a correction factor that makes the mediated coefficient from the unadjusted model comparable to the adjusted model" (Pais, 2014, p.1738); thus, differentiating the change of coefficient caused by 1) the mediation itself and 2) rescaling (Pais, 2014). Owing to the use of an ordered categorical variable for the dependent variable in the analysis, the mediation exercise was performed based on this method.

3.4.3 Ordinal Logistic Regression

Ordinal Logistic Regression (OLR) was deployed to answer research question three. As the dependent outcome that is agreeableness of achieving CSC in organisations is an ordered variable, OLR was applied. CSC has three categories; (i) agree, (ii) neutral and

(iii) disagree that governance instruments were effective in influencing CSC is achieved in organisations. All the regressions were adjusted for service tenure. Ordinal logistic regression assumes that the relationship between each pair (IV and DV) of outcome group categories are the same. This study applied the proportional odds model. The proportional odd model is mostly opted by many researchers due to its simplicity where only one regression coefficient is necessary in explaining the effect of one explanatory variable on the dependent variable resulting of one common odds ratio (Bender & Grouven, 1997, p.548).

Since the outcome variable is ordered and categorical, Bender and Grouven (1997) posited that one way to arrange the outcome variable in an orderly manner is through cumulative probabilities, cumulative odds and cumulative logits. In ordering the categories as $k+1$, the following are defined:

$$P(Y \leq i) = p_1 + \cdots p_i$$

$$odds\ (Y \leq i) = \frac{P\ (Y\ \leq\ i)}{1 - P\ (Y\ \leq i)} = \frac{p_1 + \cdots + p_1}{p_{i+1} + \cdots + p_{k+1}}$$

$$logit\ (Y \leq i) = ln\left(\frac{P(Y\ \leq i)}{1 - P(Y \leq i)}\right), i = 1, \dots k$$

Thus, the cumulative logistic model for ordinal regression is as follows:

$logit\ (Y \leq i) = \propto_i + \ \beta_{i1}X_1 + \cdots + \beta_{im}X_m, i = 1, \dots, k$ (Bender & Grouven, 1997, p.547)

This model has k model equations and one logistic coefficient β_{ij} for each category and/or co-variate combination. Hence, the general cumulative logistic regression model contains a large number of parameters (Bender & Grouven, 1997).

However, if the logistic coefficients do not depend on i, then only one common parameter β_j for each co-variate is necessary where the cumulative odds are as follows: $odds\ (Y \leq i) = \exp(\propto_i) \exp(\beta_1 X_1 + \cdots + \beta_m X_m), i = 1, \ldots, k$ (Bender & Grouven, 1997, p.547). This means that the k odds for each cut-off category i differ only with regards to the intercepts α_i; in other words, the odds are proportional (Bender & Grouven, 1997).

In this regression, an important assumption to be checked was proportional odds or parallel regression assumption (Fullerton & Xu, 2012). This assumption stated that the dependent variable's categories were parallel to each other which indicates that the relationships between the independent variables and the dependent variable were the same for the dependent variable’s categories (Fullerton & Xu, 2012). Thus, it has to be tested to ensure it is not violated. The assumption is violated if the p-value is significant (less than 0.05).

3.5 Pilot study

For the purposes of this thesis, a pilot study was conducted for data collected between the period from 21 August 2013 until 31st December 2013 where questionnaires were distributed both by hand and through online using the survey monkey software. The pilot study was conducted not only to validate the research instrument, but also provide a platform to gain important insights into the variables before administering the final survey for the full scale study. Using convenience sampling approach, 30 observations were collected and analyzed during the period of the pilot study. The observations from the pilot study was later combined with data from the main study. According to Thabane et al. (2010), data from both pilot and main study can be combined if the sampling frame and methodologies are the same. Thabane et al. (2010) also cautioned for the key features of the main study to be preserved while conducting the pilot test. Based on the results of the pilot study, the survey instrument was further refined.

3.6 Summary

This chapter presented the main framework and approaches to collect data and analyse them in answering the research questions. This chapter also discussed the justification of preferred research methodology and design in terms of sampling technique, instrument, and analytical methods. By using this approach, this study attempted to examine the behavioural intention of users to cooperate, the mediation effects of cooperation between selected organisational security practices and security compliance and finally, the effectiveness of cyber security governance instruments implemented at three different levels.

CHAPTER 4:DRIVING COOPERATIVE BEHAVIOUR IN ORGANISATIONS: THE FIRST STEP FOR CYBER SECURITY COMPLIANCE

4.1 Introduction

Most security researchers claimed that information security problem is not about technology, but focuses more on the human issue (Sasse, Brostoff, & Weirich, 2001; Schneier, 2000; Vroom & Von Solms, 2004). Apart from security breaches that were committed intentionally, Vroom and Von Solms (2004) are of the view that employees' ignorance of security policies can also contribute to security breaches. Previous security scholars have studied employees' behavioural aspect on security compliance from several social behavioural theories; such as deterrent theory (Cheng et al., 2013; Herath & Rao, 2009; Straub Jr, 1990), protection motivation theory (Vance, Siponen, & Pahnila, 2012), theory of planned behaviour (Ifinedo, 2012) and rational choice (Bulgurcu, Cavusoglu, & Benbasat, 2010; Pahnila, Siponen, & Mahmood, 2007). These studies explored factors relevant to individuals' behaviours such as user's belief, attitudes, rational beliefs and habits (Bulgurcu, Cavusoglu, & Benbasat, 2010; Pahnila, Siponen, & Mahmood, 2007), fear of sanctions (Straub Jr & Nance, 1990), the behavioural intention of an individual to perform such a given behaviour (Ifinedo, 2014) and information security climate in organisations (Goo, Yim, & Kim, 2014) that influence employees' behaviour in achieving cyber security compliance. These studies focus on users' behaviour at the organisational level. Despite the claim that people are the weakest link in the cyber security ecosystem (Bresz, 2004; Sasse, Brostoff, & Weirich, 2001; Vroom & Von Solms, 2004), little has been done to relate people's role in cyber ecosystem and their contribution towards cyber security compliance.

Using quantitative approach and BLR analytical method as discussed in sub-sections 3.3.1 and 3.4.1 respectively, this chapter seeks to answer the first research question "What are the factors that motivate users to cooperate in achieving cyber security compliance?". The factors that motivate users to cooperate in complying with cyber security compliance are namely, cyber security awareness, security role, technical capabilities and institutional role. The first three factors were derived from Theory of Planned Behaviour while the fourth based on theory of institution, both previously discussed in chapter two. Cooperation which is central to this study is derived from the non-excludable aspect of cyber security as a public good. Thus, this chapter analyses these factors that contribute to users' intention to cooperate in achieving security compliance, so that it provides a better approach in dealing with the people issue. Then, it is imperative for the information of these security requirements to be disseminated to all employees in the organisation and in return for them to extend the necessary cooperation in complying with these requirements.

Of the five sections in this chapter, section two discusses the theoretical considerations of the four factors described above followed by section three on the variable measurements. Section four presents the results of the binary logistic regressions conducted before analysis were discussed in section five. Finally, section six presents the summary of this chapter.

4.2 Theoretical Considerations

As argued in chapter one sub-section 1.3 of this thesis, cooperation has been identified as the key variable in this study. In order to investigate behavioural intention of employees to cooperate, this study adopts a suggestion made by Ajzen (1991, p. 185) where for intention of behaviour of interest to be studied, it has to be specifically defined. Thus, this leads to "intention to cooperate to achieve security compliance (ITC)" which is the first dependent variable. In predicting individuals' intention to perform a behaviour as described by Ajzen (1991), motivational factors that influence such behaviour are associated with their efforts to perform such behaviour. Thus, in this study, the explanatory variables derived from this theory are security awareness (attitude), security role (subjective norm) and technical capability (perceptive behaviour control) while cooperation was derived from the public good theory. The fourth explanatory variable (institutional role) is derived from the institutional theory by (North, 1991).

We propose two models in answering the research question 1. In the first model, we propose that security awareness, security role, technical capabilities and institutional role influence the users' intention to cooperate in promoting cyber security. Each of this is explained below. Security awareness may have an effect on employee's ITC through their beliefs whereas security role within an organisation can influence ITC through the subjective norms. By subjective norm is meant social pressure on individuals either to perform or refrain from such cooperative behaviour. The importance of this variable is related to perceived importance of employees to cooperate in complying with security requirements which is internalised via top management. Top management was thus, pressured by the sector leads in adhering to directives and policies issued by the central authorities. The governance structure of CNII defines the role of sector lead as an institution that includes regulating, monitoring and implementing cyber security programmes in each sector. Technical capability refers to perceived behavioural control which comprises technical security expertise and technical information that may affect ITC in organisations in adhering to security requirements. Institutional role refers to the role played by sector leads in providing cyber security guidance through circulations or policies to CNII organisations.

In addition, ITC predicts whether actual cooperative behaviour can be obtained, resulting in the second dependent variable which is our second model. Cooperative behaviour indicates the willingness and voluntary aspect of such behaviour in meeting a common goal (Viki et al., 2006).

Following the above discussion, the analytical framework is presented in Figure 4.1 below. Control variables are discussed in sub-section 4.3.6.

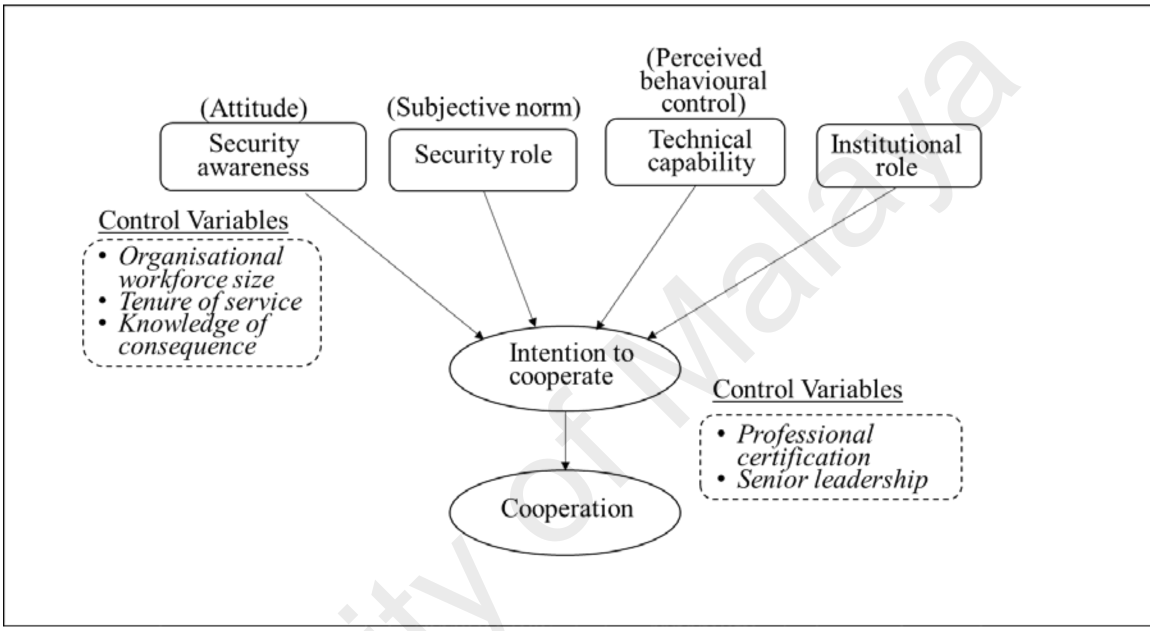


Figure 4.1: Analytical Framework for Behavioural Factors that Contribute to Cooperation
Source: Author

4.2.1 Intention to Cooperate and Cooperative Behaviour

Some studies have linked ITC with compliance achievement. Murphy, Tyler, and Curtis (2009), asserted that fair treatment and legitimate laws and values can make people cooperate to improve their compliant behaviour. Studies related to behavioural intention to cooperate with the police produced results that vary (Tyler & Fagan, 2008; Viki et al., 2006). Tyler and Fagan (2008), posited that the public will only cooperate to report crimes if they know that the enforcement e.g. police is the legitimate party for them to do such reporting. Although Viki et al. (2006) found that race was a determinant for public's willingness to cooperate in giving witness statement in court, it was not significant in reporting incidents to the police. Meanwhile, to understand taxpayers' intention to comply with income tax filing, Langham, Paulsen, and Härtel (2012) revealed that cooperation by the tax office was significant particularly in situations when volitional controls were completely absent. Langham, Paulsen, and Härtel (2012), further added that the obstacles faced by taxpayers to do tax filing such as filling up relevant forms (that could be complicated to them) could be minimized if the tax office was cooperative to assist.

Intention has been discussed as a precursor to the actual behaviour (Ajzen, 1985, 1991). Previous studies have shown that behavioural intentions have frequently led to the actual behaviour itself. These studies include intentional behaviour on cooperation (Jeffries & Becker, 2008) and also studies related to security compliance behaviour (Pahnila, Siponen, & Mahmood, 2007; Siponen, Mahmood, & Pahnila, 2014; Siponen, Pahnila, & Mahmood, 2010).

4.2.2 Security Awareness

One big challenge of implementing security initiatives was to make individuals at all levels in an organisation understand and feel the significance of security and diminish negative perceptions that security initiatives were burdensome. A study by Hu, Hart, and Cooke (2007) indicated how security procedures introduced in organisations have affected work routines contributing to inefficiency in organisations. This indicates lack of awareness in understanding the criticality of security procedures that can affect attitude towards security.

Security researchers agreed that attitude towards information security behaviour can be shaped through information security awareness programmes (Bulgurcu, Cavusoglu, & Benbasat, 2010; Ifinedo, 2014; Safa et al., 2015; Siponen, 2000). Since awareness programmes are able to motivate users to adhere to security requirements, they should naturally be prescriptive in nature (Siponen, 2000) to ensure that users will not only learn to protect information but also avoid being victims of social engineering attacks. Users' participation and social bonds created through awareness sessions can influence users to comply with security policies and procedures (Ifinedo, 2014). Safa et al. (2015), demonstrated how awareness is able to change users' attitudes towards information security through knowledge acquisition from these programmes. For easy absorption, the process should be continuous and consistent (Siponen, 2000).

The extent of security requirements communicated to employees affects the level of cooperation to comply. Not only asymmetric information causes security implementation gap, but also creates opportunistic behaviour (Mulej, Rebernik, & Bradac, 2006). Thus, cooperation is not possible when information is not appropriately exchanged. For security awareness programmes to be effective, not only they have to be consistent but to be effectively communicated in organisations.

In an experiment conducted by Jerdee and Rosen (1974), communication played a significant role to create socially responsible norms for group members to produce behaviour that benefits them all. Their study exhibits the significance of having members in groups to provide commitments for them "to act in a socially responsible manner as a means of producing behaviour in the common interest" (Jerdee & Rosen, 1974, p.716). In a different context, effective communication was identified as one of the factors to be incorporated in the school policy to improve students' behaviour against bullying (Sharp & Smith, 1991). This ensures that relevant practices in improving pupils' behaviour were consistently deployed to create awareness about it and how to react when bullying occurs. Effective communication is central to the success of organisational structures and processes in governing information security in organisation (Brotby, 2001, p. 12). It allows intended messages to reach the target audience in a way where they are able to comprehend; thus motivate them cooperate to perform required actions. For communication to be effective, it has to be clearly and successfully delivered, received and understood by the recipients (Folske-Starlin, 2017). Employees should be well-informed on actions to be taken (Adams & Sasse, 1999; Albrechtsen, 2007). Thus, it has to be consistent and continuous. On the other hand, a lack of communication (Adams & Sasse, 1999; Reich & Benbasat, 2000) can decrease responsiveness (Teo & Ang, 1999) in the event of security events; thus underutilize the abilities of security teams (Ahmad, Hadgkiss, & Ruighaver, 2012). In short, security awareness programmes blended with effective communications are paramount in inducing employees to act responsibly making them cooperate in responding to security efforts planned by the organisations.

4.2.3 Security Role

Subjective norms refer to social pressures exerted on individuals either to perform or not to perform a specified behaviour (Ajzen, 1991). These pressures may be derived from internal or external sources. In this study, CNII organisations are governed by the national cyber security policy and relevant directives through their sector leads (National Security Council, 2012; Zahri Yunos et al., 2010). To internalise the national security objectives, sector leads are to ensure that these directives and policies are adhered to and implemented accordingly in organisations under their purview. Organisations through their leadership pursue these objectives by setting security mission and vision for the organisation. Thus, it is the role of top management to influence subordinates' attitudes and motivate them in internalising the organisation's security objectives to achieve its vision. Internalisation can be the result of an underlying process that influences individuals to adopt an induced behaviour (Kelman, 1958). Plug, Meyer, Louw and Gouws defined internalisation (as cited in Venter, Kruger, & Herbst, 2007, p. 6) as "the process through which individuals make the values, opinions and attitudes of others part of their own belief system and act accordingly". In a study of family businesses by Venter, Kruger, and Herbst (2007), internalisation was observed as the process where culture, values and actions of the founder was instilled in businesses through multiple channels. The traits were first adopted by the top management before spreading them to the rest of the employees.

Top management is capable of providing guidance and enforcement for users to learn about security requirements and how they are best to be implemented in organisations. Apart from top management, the middle management is mainly to mediate and communicate the policies defined for implementation in organisations (Renaud & Goucher, 2012). According to Safa et al. (2015), subjective norms in organisations can be effected by security policy especially to those who have supervisory roles in organisations, where their adherence to this policy can influence others to stay alert and conscious in handling organisations assets. One of the middle management's tasks is to consistently remind their staff of the importance of information security and to adhere with security policies. Together with the IT technical team, they should also provide clear security policies for easy adoption (Siponen, Mahmood, & Pahnila, 2014). Thus, in implementing security controls in organisations, those who hold various authority roles are perceived to be of importance in influencing peers and subordinates to cooperate with the organisation to achieve security compliance.

4.2.4 Technical Capabilities

Cooperation for people in groups are important for collective action to succeed. In making reference to previous literature (Agrawal, 2002; Bardhan, 1993), Araral (2009) made a point that it will be a challenge to achieve cooperation when resources are too much or too little. In this study, resources which are in the context of cyber security technical competence and capabilities have a profound impact for organisations to achieve cyber security compliance. Technical capabilities refer to availability of technical skills and competence not only in managing systems and platforms but also in leveraging security information e.g. vulnerabilities and threats to secure operations. The growing needs of these groups require organisations to invest in various security disciplines (Furnell, Fischer, & Finch, 2017). Technical skills and know-how in designing, operating and maintaining information systems are as critical as managing security risks. Apart from having security controls in place, hiring competent and skilled technical personnel is also crucial to ensure that the deployment meets both, security and return of investment objectives (Musa, 2012). An experiment conducted by Furnell et al. (2018), shows that support and guided users in password selection and usage can reduce the choice of weak passwords that can contribute to security breaches. The security team should be able to make sense of security information pertaining to the technologies deployed and convey accurate information to users for them to fully understand and how to use the systems effectively (Da Veiga & Eloff, 2010; Musa, 2012).

4.2.5 Institutional Role

Previous security scholars (Cavusoglu et al., 2015; Hu, Hart, & Cooke, 2007; Kwon & Johnson, 2011) had acknowledged the role of institutions as important regulators in cyber security initiatives. In the Malaysian ecosystem, this study observes the importance of CNII sectors leads in ensuring security measures are implemented in organisations under their purview; thus, influencing their employees to collectively work in meeting the national security policy objectives (National Security Council, 2012). The cabinet directive[5] issued by the Malaysian Cabinet on ISMS implementation in 2010 and National Security Council (NSC) Directive No 24 issued by the National Security Council in 2012 served as the main factors in driving security efforts in CNII sectors in Malaysia. While the former requires CNII organisations to implement the ISMS and later be certified to

[5] This cabinet directive is discussed in details in sub-section 1.2.2.2

ensure cyber threats and risks are managed prudently, the latter provides guiding principles to secure CNII organisations among others comply with ISMS, BCM implementation, establishment of Computer Emergency Response Team (CERT), capabilities and procedure. Establishment of a CERT team in CNII organisations is part of the National Cyber Crisis Management framework that requires cooperation in these sectors in managing cyber security incidents before it becomes a crisis to the country (National Security Council, 2012).

Thus, the role of institutions in cyber security is observed as the underlying determinant of a subjective norm in driving employees' conscious behaviour in dealing with cyber security. This includes guidance and circulations on cyber security efforts initiated by sector leads and the central authority.

4.3 Variable Measurements

To operationalise the constructs in answering the first research question, we adapted some items from previous relevant studies. We also developed new constructs that were not published before. For all items of the constructs, a five-point Likert scale was employed from 1= strongly disagree, 2 = disagree, 3 = neutral, 4 = agree and 5= strongly agree.

4.3.1 Security Awareness

The first explanatory variable, attitude was formed through a latent variable that comprises security awareness and communication. Validated from previous studies (Bulgurcu, Cavusoglu, & Benbasat, 2010; Da Veiga & Eloff, 2010; Safa et al., 2015), security awareness is capable of influencing employees' attitude in achieving cyber security compliance behaviour. Security awareness involves education and training (Siponen, 2000). Security awareness is also capable of establishing a trusted environment among stakeholders (Veiga & Eloff, 2007) where trust is identified as a determinant of cooperation (Jeffries & Becker, 2008; Smith, Carroll, & Ashford, 1995). Trust has also been critical in establishing a secure IT environment, where the presence of trust between management and employees is essential for the establishment of processes and management related to information security (Veiga & Eloff, 2007). Increasing trust through better predictions was associated with reducing uncertainties. In their study in the financial industry, Flowerday and Von Solms (2006) has also suggested that one of the conditions in establishing trust is through uncertainty reductions as predictability is enhanced by communicating relevant information to stakeholders via financial statements. Berger and Calabrese (1975) argued that frequency of communciation is necessary between people to reduce uncertainties about each other as this could cause change of person's opinion, beliefs and behaviours. Thus, when security issues are not communicated as and when required, it creates problem to those who are responsible for the implementation of security controls (Furnell et al., 2009).

Thus, in measuring security awareness, the variable is based on two constructs; security awareness and communication based on four items adapted from the above studies. Respondents were asked to give their level of agreeableness with four items that formed the construct: information security awareness programmes in their organisations (SA1), frequency of the awareness programmes (SA2), effective communications on security requirements (EC) and sufficient communications on security requirements (SC) in their organisations. See Appendix A section 2.

4.3.2 Security Role

This study proposes security role as a proxy to subjective norms and that this subjective norms affect ITC. Everyone is responsible to ensure information is protected and is secure in organisations. Apart from end-users, there are other groups in organisations that are provided with security roles in organisations – e.g. top management, middle management and technical management. These groups have defined roles to ensure objectives of protecting information are aligned with organisations' goals and objectives. Although statistics show that involvement of board level and top management are critical to ensure data breach is effectively attended to in organisations (Ponemon Institute, 2015), middle management has also been observed to serve both levels; top management and technical team. Its main role is to ensure that cyber security policies and procedures are implemented and enforced by relevant stakeholders in the organisation (Kritzinger & Smith, 2008). These are the group of management who deals with daily security matters and work with the technical team and the rest of employees ensuring cooperation to be obtained for information security programmes to be delivered. But, at the same time the middle management also needs to assure that objectives set by their top management is achieved. The final category is the technical management team which ensures that all aspects of security controls such as vulnerabilities were correctly implemented and consistently monitored (Kritzinger & Smith, 2008).

For this study, the security role variable is measured based on demographic information and its inclusion is necessary to understand whether this variable has any effect on the dependent variable. Data on security role was captured in four categories, top management, middle management, technical operations and other roles. For a better interpretation of the analysis the categories were collapsed into three: 1= top management, 2 = middle management and 3 = technical. Respondents who were in "others" category were included in the middle management category. The rationale is that those from other categories were relatively relevant of performing the middle management tasks. See Appendix A section 1. To understand the organisational outcome, many researchers used organisation demographic characteristics such as education level, tenure of service and workforce size in their studies (Smith et al., 1994).

4.3.3 Technical Capabilities

Several scholars (Leonard, Cronan, & Kreie, 2004; Madden, Ellen, & Ajzen, 1992) did not measure PBC since they did not see its necessity where the behaviour in question was voluntary that is under volitional control. However, in this study, due to involvement of sector leads in ensuring CNII organisations adhere to national directives and guidelines, employees in these organisations were no longer under a full volitional control. As such, we feel that PBC is necessary to ease employees' efforts in paving their way to perform security related tasks. In referring skills and competence as PBC, Siponen (2000) posited that these elements can make adherence to security guidelines a simple task. Thus, we measure respondents' PBC concerning ITC using technical capability (TC) as a mechanism to influence the degree of easiness or difficulties in performing the intended behaviour. Triandis argued (as cited in Taylor & Todd, 1995, p. 139), that availability of resources and opportunities is important to facilitate conditions for individuals to perform such behaviour.

For the assessment of TC, respondents were asked to indicate the extent of their agreeableness on technical related capabilities comprising security expertise and information including; benefits of technical security controls (Furnell et al., 2009; Mohammed, Mariani, & Mohammed, 2015), deployment security defence tools and employment of competent cyber security experts (Ben-Asher & Gonzalez, 2015; Furnell et al., 2009), usefulness of security information from external sources to minimise successful attacks (Jerman-Blažič, 2008), sharing of technical security information on the Internet and its non-exclusivity (Rosenzweig, 2012) and sharing of information security incidents (Gordon, Loeb, & Lucyshyn, 2002; Gordon, Loeb, & Lucyshyn, 2003). Thus, the explanatory variable of TC refers to three components, first, capability of organisation through deployment of security tools (TC1 and TC2), second, available security competency (TC3) and third, security information sources to be used by the technical team (TIS1, TIS2, TIS3 and TIS4). See Appendix A section two. Technical competency is important to ensure that technical safeguards are accurately deployed in organisations (Kritzinger & Smith, 2008).

Thus, having technical capabilities gives an opportunity for the employees to understand security implementation and thus willingly to cooperate in adhering to security requirements.

4.3.4 Institutional Role

Since this study focuses on the critical sectors, we use the National Cyber Security Policy (NCSP) (Ministry of Science Technology and Innovation, July 2006) as the umbrella policy as well as NSC 24 and Cabinet directive (CyberSecurity Malaysia, 2011; National Security Council, 2012) for the CNII sectors to adhere with. This led to the next explanatory variable namely role of institutions pertaining to cyber security in CNII sectors. Through NCSP and relevant directives and sector leads, employees believe that these respected institutions would expect employees in CNII organisations to cooperate in adhering to security requirements.

This variable was operationalised as a single item variable. Respondents were asked to indicate their level of their agreeableness of sufficiency cyber security guidance provided by their sector lead (SLR). See Appendix A section two. This item was developed based on the regulatory role in accordance to the governance structure of the CNII sectors (National Security Council, 2012). CNII organisations report directly to their respective sector lead that provide relevant guidance e.g. directives and circulars in protecting their sectors.

4.3.5 Intention to Cooperate and Cooperation

Finally, there are two dependent variables; intention to cooperate and cooperation which are adapted based on a study by Jeffries and Becker (2008) but deployed in a different context and setting. Jeffries and Becker (2008), analysed trust aspects in influencing cooperation while this study examined security practices as factors that contribute to behavioural intention to cooperate. For this study, both variables are measured as single items. The first dependent variable was measured by asking respondents to state their level of agreeableness whether they have the intention to cooperate with the organisation in security programmes to achieve compliance (ITC). See Appendix A section two. The second dependent variable was determined by asking respondents the level of cooperation achieved in their organisations based on a single item (CB). The item was measured based on a five-item Likert scale: 1 = very low, 2 = low, 3 = moderate, 4 = high and 5 = very high. See Appendix A section two. In a study on information security conducted by Vance, Siponen, and Pahnila (2012), single-item measures were also included as part of their measurement items in addition to latent constructs. Although researchers were advised to use multiple-item scale (Churchill, 1979), Rossiter (2002) argued that a single-item measure is acceptable if the object of construct is conceptualised as singular and respondents clearly understand the single characteristic referred in the construct. (Bergkvist & Rossiter, 2007, 2009) further added that single-item measures can even produce high predictive validity if they were crafted carefully.

4.3.6 Control variables

There are three control variables namely, organisational workforce size, tenure of service and knowledge of consequences of loss of information attributes used for model 1. For model 2, two control variables used were professional certification and senior leadership. These were included as control variables because of their potential influence on ITC and subsequently contribute to cooperation. The effect of awareness, security role, technical capability and institutional role will be evaluated for the controlling effect of these variables in model 1. As for model 2, the effect of ITC will be evaluated for the controlling effect of professional certification and senior leadership.

It is evident that a larger group size had adverse effects on a team's coordination and communication. According to Isaac and Walker (1988), size does matter for cooperation to be achieved as people tend to be opportunist when they are in bigger groups. Thus, organisational workforce size was tested to control the model. In this study, the control variable is based on demographic data with five categories that was later collapsed to two categories coded as 1 = more than 500 and 2 = less than or equal to 500 employees. See Appendix A section 1. Tenure of service was measured by the length of time the respondents served the organisation. This variable is based on demographic data with four categories, first, less than 2 years, second, between 2 to 5 years, third, between 6 to10 years and fourth, more than 10 years. See Appendix A section 1. The shorter the tenure, the more time was needed by employees to familiarize security practices; thus cooperative intention is crucial in this phase.

Employees should have the knowledge on the undesirable consequences when there is a loss of three main attributes of information: confidentiality, integrity and availability of information as they perform their tasks. When employees know the impact of loss of these information attributes due to security breaches, they tend to work collectively to preserve the attributes. Thus, for this control variable, a construct was established based on six items; three relate to availability (AVA1, AVA2, AVA3 and AVA4), one relate to integrity (INT1) and confidentiality (CON1) respectively. See Appendix A section 2. We adapt this construct based on employees' awareness of consequences where security policies are violated (Yazdanmehr & Wang, 2016).

As for model 2 currently see Figure 4.1, the effect of ITC will be evaluated based on the effects of the control variables; professional certification and senior leadership. Professional certification is one of the benchmarks to measure competency level in organisations. Professional certification is mainly sought to increase professional credibility and improve marketability (Stinnett, 2017). The certification is very much dependent on the job portfolio. The demographic data used for this control variable was initially six categories, but was later collapsed to 2 categories: 1 = have professional certification and 0 = do not have professional certification in information security. The final control variable is the senior leadership who have responsibility of the cyber security function in organisations. They are normally addressed as CISO, CIO and frequently is part of the top management team. Their main roles are to drive the strategic agenda for information security and facilitate its strategic alignment with organisational objectives (Kayworth & Whitten, 2010). For this variable, this study used a single-item variable (CSL).   See Appendix A section 2.

4.4 Results

In answering the research question one, the analysis are divided into two types; descriptive and statistical analysis. Descriptive analysis includes demographic, normality and reliability analysis while the statistical analysis discusses the results of the multiple logistic regression conducted.

4.4.1 Data Collection Results

Questionnaires were distributed to 220 potential respondents from 21 August 2013 until 31 July 2015 where 89% was collected electronically and the remainder was collected through hard copies distribution which was later entered into the system. The questionnaires were returned with a response rate of 73%. This response rate is also acceptable as it is higher than the average response rate at 55.6%. This rate exceeds the average response rate of 55.6% that was based on a comparative study undertaken by Baruch (1999) using 175 cases from three volumes of five reputable journals and 51% on average from social studies (Pinsonneault & Kraemer, 1993).

Collecting information security related data is considered as sensitive in many organisations (Kotulic & Clark, 2004; Safa, Von Solms, & Furnell, 2016). However, out of 162 observations collected, we dropped 7 observations due to incomplete data leaving our final sample size to 155 which is higher than 150 as an acceptable sample size indicated by Anderson and Gerbing (1988). Due to challenges faced in getting respondents to participate and reveal information security practices in their organisations, this sample size is acceptable in similar studies conducted (Chan, Woon, & Kankanhalli, 2005; Ifinedo, 2012, 2014).

The results show that there are items that have missing data up to the maximum of 16%. As suggested by Little and Rubin (2002) missing values up to 20% is acceptable for analysis.

4.4.2 Sample characteristics

The demographic characteristics of the sample are illustrated in Figure 4.2. The top three respondents were those from the government (35.5%), education (20.0%), finance and banking and information and communication (both are at 13.5%) sectors. Most of the respondents served in the government and government agencies (71%) instead of private sector (29%). Respondents from workforce size of more than 500 employees accounted for 74.2% and 25.5% are those with less than and equal to 500. In our sample, 36.1% of the respondents had professional certification compared to those who did not (63.9%). Highest qualification respondents comprised of bachelor and diploma (60%), masters (27.7%) and phd (12.3%). Respondents who had served more than 10 years made up

38.7 % of the sample followed by those who had served between 6-10 years (29%), between 2-5 years (18.1%) and less than 2 years (14.2%). In security role category, the highest contributor is from the middle management (51.6%) followed by technical personnel (33.5%) and top management (14.8%). In terms of specific job portfolio, the highest contributor were those from the ICT security category (49%) followed by ICT operations (27.7%) and other portfolios comprising ICT planning, risk management and other business unit (23.2%).

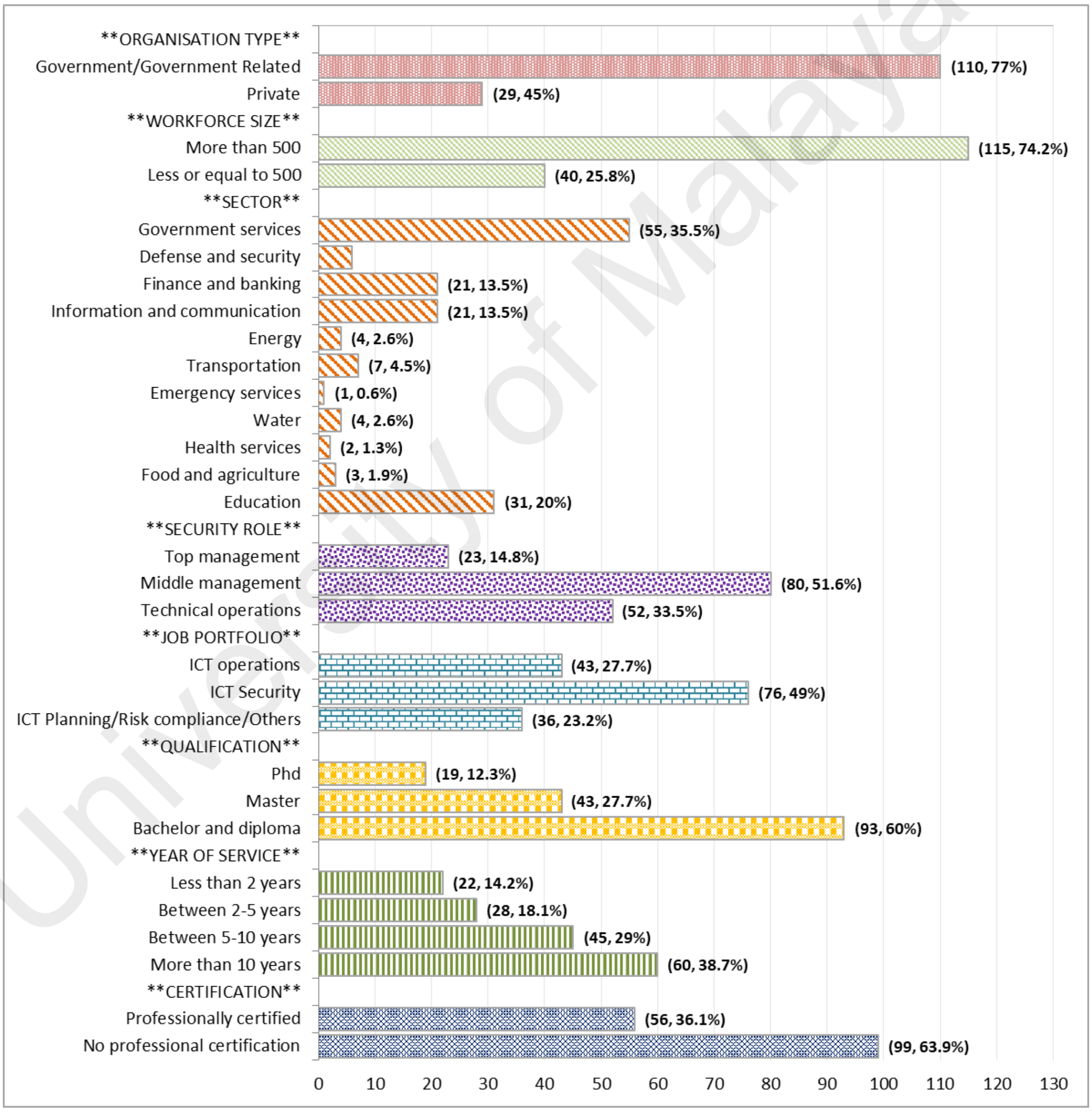


Figure 4.2: Demographic Statistics of Respondents
Source: Computed from Author’s Survey

4.4.3 Descriptive Analysis of Variables

In this chapter, two dependent variables were developed as the outcomes, “intention to cooperate” for model 1 and “cooperation” for model 2. For model 1, the dependent variable is coded with 1 representing “have intention to cooperate” and 0 otherwise. For model 2, the dependent variable is coded with 1 representing “cooperation” and 2 otherwise. Explanatory variables are discussed in sub-section 4.3.1 to 4.3.4. The descriptive analysis of the variables are tabled in Table 4.1.

Table 4.1: Descriptive Analysis of Dependent, Independent and Control Variables for Multiple Logistic Regression Model

Variables	n,(%)
Intention to cooperate [a]	155, (100.0%)
Have intention to cooperate	92, (59.4%)
No intention to cooperate	63, (40.6%)
Cooperation [a]	155, (100.0%)
Cooperative	139, (89.7%)
Non-cooperative	16, (10.3%)
Security awareness [c]	155, (100.0%)
Security role	155, (100.0%)
Top management	23, (14.8%)
Middle management	80, (51.6%)
Technical management	52, (33.5%)
Technical capabilities [b]	155, (100.0%)
Institutional role [b]	155, (100.0)
Knowledge of consequences of security breach [b]	152, (98.2%)
Organisational workforce size [a]	155, (100.0%)
> 500	115, (74.2%)
<= 500	40, (25.8%)
Tenure of service	155, (100.0%)
Less than 2 years	22 (14.2%)
Between 2-5 years	28 (18.1%)
Between 5-10 years	45 (29.0%)
More than 10 years	60 (38.7%)
Senior leadership [b]	155, (100.0%)
Professional certification [a]	155, (100.0%)
Have IS professional certification	56, (36.1%)
No IS professional certification	99, (63.9%)

Note of Table 4.1 :

n-total observations,
[a] Intention to cooperate, cooperation, organisational workforce size and professional certification were measured as a dummy variable
[b,c] These independent variables were measured by the Likert scale (from 1=strongly disagree to 5=strongly agree)
Source: Computed from author's survey

4.4.4 Data Normality Analysis

Based on Jarque-Bera test conducted, the results showed that only one variable, i.e. effective security awareness was normally distributed with a Jarque-Bera statistics value of 4.47, 0.5 > p > 0.1 indicating that the other variables were not normally distributed [6]. Thus, the null hypothesis is rejected. Because the data was not normally distributed, it did not meet the assumption for linear regression testing. Hence, we used BLR to analyze the data.

4.4.5 Reliability Analysis

The results show that the computed Cronbach values for constructs of model 1, institutional role and knowledge of consequences are 0.711 and 0.705 respectively[7]. For security awareness construct, the initial Cronbach value was less than 0.7, but was later improved to 0.702 by dropping one item (SC). Similarly, for technical capabilities, the initial Cronbach value for eight items was below 0.7. By dropping three items (TIS1, TIS3 and TIS4), the value was improved to 0.728. Therefore, all constructs have values above 0.7 which are acceptable (Nunnally, 1978). For model 2, only single item variables were used to predict the outcome variable, thus, no Cronbach values were computed.

[6] Data normality method was discussed in sub-section 3.3.1.5
[7] Reliability test method was discussed in sub-section 3.3.1.6

This regression model was later tested for multi-collinearity effect using Variance Inflation Factor (VIF) where estimates of the VIF were between 1.058 to 1.194 for model 1 and between 1.005 to 1.016 for model 2 for all variables that did not exceed 10; suggesting there was no multi-collinearity present in the overall models (Marquaridt, 1970). The details of the VIF for model 1 and model 2 are reflected in Table 4.6 and Table 4.7 respectively.

4.4.6 Model Goodness of Fit Test: Hosmer and Lemeshow

In BLR, Hosmer and Lemeshow test was assessed to test how well the data fits the model by assessing how close the observed and predicted events match. The null hypothesis suggests that "the model fits" will be rejected if the p-value is less than .05. For the model goodness of fit test, Hosmer and Lemeshow test results are presented in Table 4.2 and Table 4.3 for model 1 and model 2 respectively. The null hypothesis of "the model fits" is accepted where the model is good fit to the data, and rejected where the model is not fit to the data, where the p value < .05. Model 1 suggests that the model fit the data well ($\chi 2 = 9.051$, p = .338) since it produces insignificant chi square (where p > .05). Similarly, model 2 also indicates fit to data ($\chi 2 = 2.642$, p = .916) and produces insignificant chi square, where p > .05.

Table 4.2: Hosmer and Lemeshow Test (model 1)

Hosmer and Lemeshow Test			
Step	Chi-square	df	Sig.
1	9.051	8	.338

Table 4.3: Hosmer and Lemeshow Test (model 2)

Hosmer and Lemeshow Test			
Step	Chi-square	df	Sig.
1	2.642	8	.916

4.4.7 Omnibus Test of Model Coefficients

Omnibus test of model coefficients was used to check if the model is better with predictors (with explanatory variables included) than the one without predictors (the baseline model). The results of the Omnibus test of model coefficients as presented in Table 4.4 for model 1 shows that the model with predictors was significantly better than the model without predictors ($\chi 2$ = 34.692, df = 10, p < .05). The model Chi-Square, 34.692 is the value of the difference between the -2LL for a model with only one constant (206.248) with no predictors and the 2LL for the model for the model with predictors (-2 Log likelihood value of 171.556). This shows that the model containing predictors is a significant improvement over the model with just a constant.

Table 4.4: Omnibus Tests of Model Coefficients (model 1)

Omnibus Tests of Model Coefficients

	Step	Chi-square	df	Sig.
Step 1	Step	34.692	10	.000
	Block	34.692	10	.000
	Model	34.692	10	.000

Similarly, the coefficients for model 2 as presented in Table 4.5 indicated that the model with predictors was significantly better than the model without predictors ($\chi 2$ = 23.152, df = 5, p < .05). The model Chi-Square, 26.712 is the value of the difference between the -2LL for a model with only one constant (102.956) and the 2LL for the model for the model with predictors (-2 Log likelihood value of 76.244).

Table 4.5: Omnibus Tests of Model Coefficients (model 2)

Omnibus Tests of Model Coefficients

	Step	Chi-square	df	Sig.
Step 1	Step	26.712	5	.000
	Block	26.712	5	.000
	Model	26.712	5	.000

4.4.8 Results of Binary Logistic Regression

Two regression models were produced. In the first model, the dependent variable was the ITC while cooperation was the dependent variable for the second model. In the first model, the results show that security awareness, security role, and institutional role were significant predictors that influenced employees' ITC (see Table 4.6).

Table 4.6: Determinants of Intention to Cooperate by Means of Binary Logic Regression (model 1)

Variables	Coefficients, β	Std. Error (S.E.)	Odds Ratio (OR)	Var. Inflation Factor, (VIF)	95% Confidence Interval	
					Lower Bound	Upper Bound
Security awareness	0.940***	.331	2.561	1.062	1.339	4.898
Security role				1.058		
Top management	1.171**	.622	3.224		.954	10.920
Middle management	1.015**	.437	2.759		1.171	6.498
Technical and others	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)
Technical capabilities	-.170	.243	.843	1.147	.524	1.358
Institutional role	.424**	.211	1.528	1.111	1.011	2.308
Organisational workforce size				1.090		
> 500	-1.074**	.483	.342		.133	.880
<= 500	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)
Tenure of service				1.194		
Less than 2 years	1.276**	.722	3.581		.870	14.742
Between 2-5 years	-.640	.586	.527		.167	1.664
Between 5-10 years	-.233	.485	.792		.306	2.048
More than 10 years	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)
Knowledge on consequences of security breach	-0.082	0.338	0.921	1.079	0.448	1.895
Constant	-3.253	2.378	1.872			

Note: ***, ** - Significant at 1% and 5% respectively, ref.- reference category

Source: Computed from Author's Survey

The co-efficient of security awareness (.940) is significant at 1% significance level and positive, suggests that increasing security awareness is positively associated with increased log odds of ITC (OR:2.561; 95% CI: 1.339, 4.898) by .940 times. The OR indicates that for every 1 unit increase of security awareness, the likelihood that ITC is displayed increases by approximately 2.561.

Holding the technical category as the reference group in the binary logistic analysis (OR = 1.00), the top and middle management illustrated significant association with ITC. The results revealed that coefficients of top management (1.171) and middle management (1.015) were both significant at 5% significance level respectively and positive. An increase of security role at the top management level increases the odds of displaying ITC by 1.171 times (OR:3.224; 95% CI: .954, 10.920), while at the middle management level, an increase of one employee with security role at this level increases the logs odds of displaying ITC by 1.015 times (OR: 2.759; 95% CI: 1.171, 6.498). This support findings by Cooper (2006) that top management is more influential than the middle management in exerting behaviour in organisations. The ORs for those who hold security role at the top management and middle management are 3.224 and 2.759 respectively. This indicates that the odds that top management displayed ITC towards security compliance is 3.224 times more compared to those at the technical level. Similarly the OR for middle management group shows that the odds that this group displayed ITC 2.759 is times more compared to those at the technical level. The results of this study are consistent with Kabay (1994) that those who had security roles in organisations were capable of convincing employees to cooperate in improving security practices in organisations. However, technical capabilities are found not to be significant in predicting employees' ITC to achieve security compliance. This can be due to lack of competence since there is only 36.1% have relevant cyber security certifications in our sample.

The co-efficient of institutional role (.424) was significant at 5% significance level and positive, indicates that sufficient guidance and directives on cyber security was positively associated with the log odds of ITC (OR:1.528; 95% CI: 1.011, 2.308). The OR explains that for every 1 unit of institutional role demonstrated by the central authority and sector leads, the likelihood that ITC is displayed towards achieving security compliance increases by approximately 1.528. Since security awareness (attitudes) and security roles (subjective norm) and institutional role (subjective norm) are significantly found to predict ITC, the results of this study are consistent with previous findings (Ifinedo, 2012; Leonard, Cronan, & Kreie, 2004; Siponen, Mahmood, & Pahnila, 2014) where attitudes and subjective norm were found to be significant in predicting behavioural intention.

The results also revealed interesting findings of the control variables where organisational workforce size and tenure of service showed significant effects. Firstly, there is an inverse relationship between the organizational workforce size and ITC. The results show that an increase of one employee in one organisation reduces the log odds of displaying ITC by 1.074 indicating that there could be possible opportunistic behaviour developed in large groups (OR: .342; 95% CI: .133, .880). The OR indicates that the odds that employees established ITC towards security compliance is .342 more in large organisations compared to smaller ones. Secondly, an increase of one employee with tenure less than 2 years increased the log odds to establish ITC by 1.276 times (OR: 3.581; 95% CI: .870, 14.742). The results also show that the likelihood of OR of those who have served their organisations less than 2 years is 3.581 times higher in establishing ITC compared to those who have served more than 10 years. This shows that being newcomers, they were still in a learning phase to understand the security culture and values of the newly joined organization; thus, they were willing to cooperate more. These findings are supported by McNeil and Thompson (1971) where close monitoring were needed for newcomers since they were not familiar with the organisation’s activities. Also, the results did not suffer from endogeneity problems as the constant is not significant.

Based on the results, the relative effects of factors in model 1 can be summarised by the following logistic regression equation:

$$\begin{aligned} logit\left(\frac{\hat{p}}{1-\hat{p}}\right) &= -3.253 + 0.940(Security\ awareness) \\ &+ 1.171(top\ management) + 1.015\ (middle\ management) \\ &+ 0.424(institutional\ role\ ) \end{aligned}$$

where, p is the probability that a respondent has the intention to cooperate; 1 – p is the probability that a respondent has no intention to cooperate; $p/(1 - p)$ is the odds that a respondent has the intention to cooperate.

Meanwhile, the results of the second model show that ITC is the significant predictor to achieve cooperation (see Table 4.7). The co-efficient of ITC (2.701) was significant at 1% significance level and positive, indicating that increasing ITC was positively associated with increased log odds of cooperation among employees in the organization by 2.701 times (OR: 0.067; 95% CI: .014, .331). The OR for ITC is .067, which indicates that for every 1 unit of ITC displayed, the likelihood that cooperative behaviour is achieved increases by approximately .067 times. As for control variables of professional certification and senior management who in charge of cyber security, only the latter is found to be significant in controlling the model. To have someone at the senior management level in driving security initiatives in organisations can influence the rest of employees to cooperate in internalising the security efforts. Again the constant of model 2 was not significant, indicating that there was no endogeneity issue in this model.

Table 4.7: Determinants of Cooperation by Means of Binary Logic Regression (model 2)

Variables	**Coefficients , β**	**Std. Error (S.E.)**	**Odds Ratio (OR)**	**Var. Inflation Factor, (VIF)**	**95% Confidence Interval**	
					Lower Bound	**Upper Bound**
Intention to cooperate	2.701 ***	.814	.067	1.011	.014	.331
Information security (IS) professional certification				1.016		
Have IS professional certification	1.357	.815	3.885		.786	19.199
No IS professional certification	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)	(ref.)
Senior leadership in cyber security	.587**	.241	1.782	1.005	1.112	2.856
Constant	1.598	1.982	2.648			

Note: ***, ** - Significant at 1%, 5%, ref.- reference category
Source: Computed from the Author's Survey

Meanwhile, the equation for model 2 can be written as follows:

$$logit\left(\frac{\hat{p}}{1-\hat{p}}\right) = 1.598 + 2.701(Intention\ to\ Cooperate)$$

, where, p is the probability that cooperation is achieved; $1 - p$ is the probability that cooperation is not achieved; $p/(1-p)$ is the odds that cooperation is achieved in organisations.

4.5 Discussion

4.5.1 Security Awareness and Intention to Cooperate

Security awareness held in organisations can significantly instil social norms for users to co-operate in complying with security requirements. The results are consistent with previous studies (Bresz, 2004; Safa et al., 2015) that security awareness held in organisations is capable to influence individuals' behaviour to be more careful in information security; thus influence them to comply with security policies and procedures and other requirements.

Previous studies (Albrechtsen & Hovden, 2010; Siponen, 2000) also show that active participation by end-users in information security programmes and discussions held by organisations motivate them to cooperate. Security awareness programmes provides a social embededness platform that allows end-users to interact with each other, as well as with those who are responsible for security issues. Such interactions can also strengthen a sense of belongingness that make end-users feel that they are actually part of the decision-making process and aware of the consequences that will affect them (Siponen, 2000). This results for end-users to have greater sense of commitment by changing their cognitive state in believing the actual reason why they need to comply with security requirements. In this context, end-users do not think selfishly about themselves which is one main characteristic of a free-rider but, instead collectively cooperate in contributing to the compliance in order to achieve the intended security objectives of the organisation. This way end-users will realise that free riding is unavoidable in the provision of a public good but will become collectively responsible to ensure compliance is achieved.

Security awareness programmes are one of the platforms that can positively influence cooperation amongst users. These programmes should should also include incorporation of training modules that are embedded as part of the awareness approach. It provides a social embeddedness platform not only amongst users but also between users and training providers to participate and interact on security knowledge and issues. According to Ifinedo (2014), users' participation indeed create social bonds that influence users in complying with security policies and procedures; eventually increasing relationship amongst them in organisations.

In inculcating security culture in organisations, security awareness programmes have to be designed with different roles and responsibilities in the organisation. There are four categories of personnel in organisations, viz., top management who are normally the decision makers who provide the commitment and resources, middle management who implement policies, technical personnel who deal with technical aspects of security implementation and maintenance, and finally the end-users who use the systems in their day-to-day work and activities. These groups have security objectives defined within their context of responsibilities (International Organization for Standardization, 2013). Specific security awareness programmes need to be tailored to each group to ensure that the right messages can go across these personnel. For example, for the top management, an awareness session is critical to make them understand cyber security threats and their potential impact to organisations to attract their attention so that they will commit the resources to bolster security operations (Ashenden, 2008; ISACA, 2011).

Security awareness programmes are also capable of transforming those who work for their own self-interest to be part of the group to meet the mutual benefits. Apart from being known as free riders, those who work for their own self-interest are also referred to as individualists who are emotionally independent in their organisations (Hofstede, 1980). Liden, Sparrowe, and Wayne (1997), claimed that self-interest behaviour (which is the obvious trait of a free-rider) can be transformed into a group focus-oriented attitude that can provide mutual benefits. In this case, cooperative behaviour can be observed through the increase of relationship in groups.

The “people” aspect has been emphasised by massive security scholars as the problem in security (Bresz, 2004; Vroom & Von Solms, 2004). Their contributions to the organisation are measured through how much they are aware and educated as users (Eminağaoğlu, Uçar, & Eren, 2009). Although Eminağaoğlu, Uçar, and Eren (2009) proved that security programmes increased the usage of strong passwords in organisations, this improved security measures do not reflect the overall security performance in any organisation.

In ensuring information security culture being inculcated in the organisations, awareness programmes should be held consistently as this will not only cater for those who are newly employed, but also to refresh existing employees on new security requirements in organisations. Frequent and continuous awareness programmes can create social embeddedness amongst members in the group that they can collectively work on to meet organisation security goals (Rantos, Fysarakis, & Manifavas, 2012). For awareness programmes to be effective, users should be made aware of newly developed or approved security requirements, which should be consistently updated. Also, Siponen (2000) argued that the awareness creation process cannot be abrupt but requires a gradual process which demands frequent and continuous security programmes.

Frequent interactions among employees (who do not have kin relationship) through consistent security awareness programmes can be explained through the occurrence of cooperation. According to Trivers (1971) who came out with the theory of reciprocal altruism, when there are opportunities for the same individuals to repeatedly interact between them, then an individual who behaves altruistically to those who reciprocate the altruistic act will be favoured. In connecting this to cooperation, repeated interactions through frequent awareness programmes are capable of inducing cooperation among employees. This point is supported by Cooper (2006) that frequency of interactions between management and employees able to instil safety behaviour amongst employees in organisations.

Awareness programmes should be scheduled and communicated with employees to allow them to continuously interact and communicate with each other since time factor is also crucial in detecting opportunistic behaviour in social network embeddedness. According to Sanders et al. (2006), the longer members have known each other the greater the level of dependency between them, which could curb negative free-riding. Scheduled awareness programmes allow employees to plan and actively participate; thus creating a sense of belongingness amongst them. Employees tend to look forward to any scheduled programmes organised for them; as this provides them the opportunities to discuss security measures and issues and compare notes especially when their organisation is decentralised. Active participation by employees in information security programmes and discussions held by organisations that yield common insights of security practices (Albrechtsen & Hovden, 2010), thus requires cooperation amongst them.

Clear and definite impacts of security awareness programmes will not be felt if there are no mechanisms deployed to measure its effectiveness. Effectiveness of information security awareness should be measured to gauge the level of learning impact of employees and ensure its return of investment.

Communication is significant to influence users to participate and eventually cooperate to comply with security compliance. This is consistent with the findings of Adams and Sasse (1999) who showed that the lack of communication resulted in the underestimation of perceived security threats by users in their organisations. They further indicated that, users were not well-informed on security measures to be implemented in addition to the existing "need-to-know" policy on information. Thus, without sufficient information, it will derail employees from cooperating for effective deployment of security measures.

In relevant study conducted by Mohammed, Mariani, and Mohammed (2015) in healthcare sectors in the United States, the needs of communication on security issues and consistent monitoring on security controls were demonstrated. In order to earn cooperation amongst users in complying with security requirements, those requirements should be effectively communicated to intended recipients who in the context are the employees. The extent of security requirements being communicated to employees affect the level of cooperation for them to comply. When scarce information on security requirements reach them, they are not aware of policies and procedures that they need to adhere to: whether updated or newly approved versions. Employees should be informed of any enhancement of these documents. Thus, when employees are not well-informed on what they are required to do, it creates the gap and employees should not take the sole responsibility for any breaches that might occur when they do not have the information on what needs to be done. An effective communication of policies and procedures can influence employee cooperation in preventing and responding to security breaches.

Lack of communication of security measures and plans designed by security teams for employees to abide by will lessen the chance for them to co-operate to comply with those requirements. Effective communications have been important to ensure that the messages are relayed to intended recipients for them to respond to on what is needed from them. For communication to be effective for users to notice, creativity is essential with pictures and diagrams in conveying messages. In a study conducted by He, Johnson, and Lu (2015), it was shown that graphical content provided a better understanding for users to identify recommendations and causes of security incidents in comparison with the text alone.

Indeed, some argue that communication has the strongest effect on cooperation compared to other factors (Sally, 1995). According to Fishbein and Ajzen (as cited by Siponen, 2000), persuasive communication can shape users’ behaviour to change their beliefs. In addition to effective communication of security policies and other relevant requirements, attempts to instil the informed risks, threats and impacts on the organisation due to failure to comply should not be left out. Attempts should also be made to communicate the penalties for security breaches that can discourage deviant behaviour among users.

The findings of this study also replicate the findings of Jerdee and Rosen (1974) that the level of communication has an effect on people to cooperate. Indeed, (Jerdee & Rosen, 1974; p. 716) argued that communication periodically allows them to "establish cooperative coalitions". Their results show that the mean time to complete a cost-bid process in a high communication activity is twice the time taken in a low communication activity. They also argued that communication was significant in inducing cooperative behaviour not only in small population but also large population as suggested by Deutch and Krauss (as cited by Jerdee & Rosen, 1974). Hence, for socially responsible behaviour to protect common interests, communication is essential to establish and maintain cooperative behaviour (Isaac & Walker, 1988).

The medium of communication and how information is communicated can affect the level of co-operation among employees. With the deployment of technology that provides automation in certain security practices, organisations tend to shift the responsibility of protection to users through automation. However, without proper communication on the procedure of how-to, this practice can become a disaster. A related finding by Adams and Sasse (1999) demonstrate that rare communications of security knowledge such as securing passwords can lead to “insecure behaviour” among employees in organisations; thus defeats the purpose of its implementation. For security implementation to be effective, individual roles and responsibilities pertaining to security should be communicated to employees (Williams, 2001). One of the ways to do this is by stating information security responsibility in employees’ individual job description.

An important element that is widely discussed in information security literature is trust. Wright (2000) posited that communication and trust (as cited in Tov & Diener, 2008, p. 4) are two significant factors that contribute to cooperation particularly to those who are not close to each other. He deliberated that these two factors could foster social relationship to understand common goals and mutually agree towards achieving it which can happen through communication and trust is needed to avoid a perception that the cooperation formed is not abused.

Trust in a form of strategy can be used as a mechanism to avoid unfavourable behaviour such as opportunistic behaviour that grows in free riders (Flowerday & Von Solms, 2006). Flowerday and Von Solms (2006), further stated that for trust to be developed between two parties, it is imperative for one party to be able to predict the other's behaviour through communication so as to reduce uncertainty. They further stated that with greater reduction in the uncertainty of the other party, the more one was able to predict the vulnerable behaviour of a party to others. Hence, trust can be better established. The results of this study is also consistent with Flowerday and Von Solms (2006) that emphasize the needs of continuous communication for people in developing trust and cooperation in organisations over time. Using the Prisoner's Dilemma concept, Flowerday and Von Solms (2006) describe the discovery of trust that can be built over time. In this game theory, the amount of information known to the players (prisoners) who make a decision helps in determining the behaviour of the players. Flowerday and Von Solms (2006), pointed out that if the police continuously inform the prisoners (players) that the interrogation is ongoing that will never end, cooperation can be anticipated from these players where players learn to trust each other and eventually cooperate. In this context, when trust is developed, perceived uncertainty is reduced. In supporting this, Axelrod (1997) described (as cited in Flowerday & Von Solms, 2006, p. 91) that a pattern of cooperative behaviour develops trust over time.

Thus, consistent security awareness embedded with effective communication are capable of establishing trust that gradually enabale cooperative behaviour to persist in achieving security compliance.

4.5.2 Security Role and Intention to Cooperate

Secondly, security role also contributes to ITC. The results suggest the significance of both levels namely, top management and middle management in ensuring security objectives are met. Internalisation of normative pressures from the sector leads requires top management to define and set their security objectives in their organisation. This finding was consistent with the findings of (Knapp et al., 2006; Puhakainen & Siponen, 2010) who showed that top management plays a critical role in organisations achieving security compliance. Top management provides their commitment through participation and availability of resources. In Malaysia context, by internalising regulatory requirements set by the sector leads, top management in CNII organisations is committed to translate those requirements into organisational security policies and procedures. However, it is not practical for them to deliver security programmes and efforts due to their role which is more on strategic rather than operational. Rather the top management' strategic security objectives were translated into tasks that were delivered by the middle management. This is where the middle management play their role in bridging objectives set by top management with the rest of the employees in the organisations.

Our results also corroborate the government policy, whereby the implementation of Information Security Management Systems ISO 27001 (ISMS) as directed by the Cabinet Directive in 2010. CyberSecurity Malaysia (2011) targeted implementers mainly from the middle management in providing security planning and monitoring, though they work closely with top management and the technical personnel. According to Floyd and Wooldridge (1994), the middle management serves as the bridge between top management and the rest of employees in providing cooperation to achieve organisational performance. Birken, Lee, and Weiner (2012), emphasized that in the healthcare industry, the role of middle management is essential to fill the gap left by top managements in implementing healthcare innovation effectively. Although top management is very significant in supporting security, middle management is seen as the group of managers that create sparks for all employees in organisation for compliance and drive the change management process (Wagner & Brooke, 2007). In the cyber era where security threats change so fast, learning process should be able to capture on relevant changes associated with the cyber security landscape.

4.5.3 Institutional Role and Intention to Cooperate

Thirdly, the significance of institutional roles suggest that sector leads and central authorities have effectively assisted CNII organisations in motivating their employees to cooperate for security measures to be implemented in accordance with the directives issued. Obviously, in the financial and government sectors, relevant security initiatives such as guidelines and frameworks relevant to their sectors were continuously produced and enforced. This was to ensure that their ecosystem was safe and well-protected. However, to other sectors they normally ride on security directives initiated by MAMPU.

4.5.4 Intention to Cooperate and Cooperation

The findings clearly indicate the positive relationship between ITC and cooperation. The positive association between ITC and cooperative behaviour is supported by previous studies where behavioural intention is the precursor to actual behaviour (Jeffries & Becker, 2008; Pahnila, Siponen, & Mahmood, 2007; Quine, Rutter, & Arnold, 1998; Siponen, Mahmood, & Pahnila, 2014).

4.5.5 Free Riding and Intention to Cooperate

Being in groups, collective actions are required amongst the members of the group to contribute to something that benefits all of them. The author submits that in this case, all members are required to abide by security requirements as set forth by the organisation in order to reach the state of security which is considered as a "public good" for the organisation. Olson (1965) is of the view that in ensuring availability of public goods, simulating cooperation is necessary by controlling free riding which can be challenging with the presence of large members that can shield those individuals who free ride.

This relates to another key finding of this study that shows organisational workforce size is negatively associated with employees' ITC. This is consistent with previous studies (Albanese & Van Fleet, 1985; Schneider & Pommerehne, 1981; Wagner, 1995), as the population size increases, there is a tendency of free-riding to increase as users become ignorant to collectively contribute in meeting the group's objective. When a group size is big, noticeability of a member's contribution decreases; thus creating opportunities for members in the group to free-ride (Albanese & Van Fleet, 1985; Buchanan, 1965). On the contrary, the smaller the group, the greater the opportunity for cooperation to occur by members in a group (Wagner, 1995). The finding of this study also supports arguments of (Poteete & Ostrom, 2004; Stigler, 1974) that collective action is more efficient in smaller groups.

In associating free-riding with public goods, collective actions must exist to have the effect of benefits in contributing to the goods (Stigler, 1974). The scale of the operation of collective action depends on the number of individuals joining the group where the benefits to be gained from collective actions from members will be reduced if a member in the group does not participate (Stigler, 1974). Interestingly, Stigler (1974) further emphasized that those who do not contribute actually enjoy the benefits not for free but at a cheaper cost. As this happens, there will be a decrease in collective action participation. In order to achieve the desired result in situations when choice of individuals is involved, reducing the population size or implementing coercive rules to the population can be a good choice (Buchanan, 1965). The larger the user population in organisations, the higher the potential for users to free-ride (Albanese & Van Fleet, 1985); eventually resulting in lesser cooperation towards cyber security compliance.

In this study, cooperative behaviour is instilled by security efforts that provide social interactions such as security awareness programmes and communications of security programmes. Awareness of end-users on security requirements that are defined by organisations should be effective in minimizing user-related errors. The increased interoperability and interdependencies in organisations have created an environment where the use of ICT has made human interactions become minimal in organisations. The author submits that although this may create convenience to organisational operations, little human interactions constitute a lack of participation and cooperation in contributing to security compliance. This is supported by Mulej, Rebernik, and Bradac (2006) who argued that complex problems cannot be resolved by individuals due to limitation of human capabilities. Instead, cooperation is very much desired (Schalk & Curşeu, 2010). Since lack of participation and cooperation is a factor that triggers the likelihood of free-riding activities, the need for users to participate in security programmes and cooperate in complying with security programmes should not be underestimated.

Based on individualism-collectivism dimension raised by Hofstede (1983), this study explains the association of this dimension with cooperative behaviour. Individualism concerns personal gain while collectivism favours benefits of group interest. According to Wagner (1995, p.155),

> *"Cooperative contributions to group performance and well-being have the effect of diminishing personal resources that can be directed toward more personally satisfying pursuits. Under these circumstances, individualists are likely to prefer to avoid cooperation and instead devote their attention to the pursuit of personal gain."*

Wagner (1995), further argued that free riding is a rational choice made by individuals to avoid cooperation by not putting efforts, but at the same time expecting to share benefits produced by the group. In this context, individualism and collectivism can be regarded as another determinant for users' intention to cooperate in groups as these characteristics influence the level of participation in groups. This is demonstrated through a study conducted by Hwang and Francesco (2010), where an open electronic discussion board was established for students to participate as part of their e-learning medium; one critical finding is very much related to this study. Students who are highly individualists were less likely to participate in this learning medium (Hwang & Francesco, 2010). This provides similarities between individualists and free riders where there is lack of participation in cooperating and contributing to the board collectively as a larger group.

4.6 Summary

This chapter examined factors that contribute to cooperative behaviour in achieving security. Drawing from the Public Goods theory and the Theory of Planned Behaviour, the results show that there was a strong positive relationship between security awareness, security role, institutional role and ITC. This is demonstrated by examining factors that encouraged employees to cooperate in organisations. In a situation where people could not be excluded from gaining benefits of public goods, the alternative is to foster cooperation to prevent its abuse. As discussed in this study, the determinants for employees to cooperate were derived through security awareness, roles of institution and security role. This study shows that these factors can motivate them to act in a socially responsible manner as the means to achieve security compliance. Security awareness programmes embedded with effective communication can function as channels for employees to interact with each other to strengthen cooperation through creation of a sense of belongingness among them. Security awareness is critical to keep the focus of employees over the need to beware and to police cyber security issues.

Security responsibility both at top and middle management levels as significant predictors were able to stimulate frequent interactions in driving the security implementation and its related changes. Although top management is well-understood in providing commitment and support to ensure that information security remained effective in organisations, the role of middle management should not be underestimated. An explanation for this was that middle management were those who had frequent interactions with employees in bridging top management's intention with the rest of the employees. Both top management and middle management showed a strong relationship with the intention to cooperate on cyber security issues. Top management through their commitment and participation could foster cooperation in organisations. Meanwhile, consistent interaction between middle management (who are the implementers of cyber security programmes) and employees could induce cooperative behaviour. Such interactions help employees feel a sense of belongingness by collectively contributing towards a shared security compliance in organisations. Sense of belongingness could overpower self-interest, where through interactions employees can work collectively in meeting common security goals. This motivates reciprocity that can escalate to altruistic behaviour in achieving cyber security compliance in organisations. Efforts to build cooperation can ward off opportunists from hacking cyber security platforms. While free riding is both unavoidable and is often desirable, cooperation can prevent such avenues from being abused.

The results also show that role of institutions is positively correlated with employees' intention to cooperate in adhering to security requirements. Security directives and policy both at national and sectoral levels were internalised to CNII organisations through top management. Through their commitment, institutional role is observed to influence behavioural intentions to work together in achieving compliance. In addition, larger organisational workforce size had detrimental impact on employees' intention toward cooperation that could lead to the emergence of free riders. Inversely, a shorter tenure of less than two years in service suggested that there was better cooperation in working collectively as they lacked the familiarity to discharge their tasks.

CHAPTER 5:BRIDGING THE GAP BETWEEN ORGANISATIONAL INFORMATION SECURITY PRACTICES AND CYBER SECURITY COMPLIANCE: CAN COOPERATION PROMOTE CYBER SECURITY IN ORGANISATIONS

5.1 Introduction

The increasing dependence of organisations on technologies and with the Internet as the core channel of communication, it is fundamental for organisations to adopt organisational security practices to deter cyberattacks so as to minimize cyber security breaches. Organisational practices provide routines that can be followed by employees. According to North (1994), organisations through its structures and rules are capable of influencing users in moulding their conduct. Organisational practices are defined by Kostova (1999, p.309) as “particular ways of conducting organisational functions that have evolved over time under the influence of an organisation's history, peoples’ interests, and actions that have become institutionalized in the organisation.” Kostova (1999), further regarded organisational practices as the product of knowledge shared among employees in organisations embedded with their competency and skills that are accepted by employees in delivering their tasks.

Although research is abundant, there is still little insight into how cooperation fits into organisational practices in achieving security compliance. We argue that mere understanding of human behaviour is not sufficient to understand how compliance is achieved in organisations. The underlying factors of human behaviour that link organisational practices with security compliance need to be fully understood. Since cyber security is everyone’s responsibility in organisations (Williams, 2008; Wylder, 2003), we argue that cooperation is the underlying factor that influences organisational practices to strengthen security compliance.

Thus, this study attempts to explore the intervention of cooperation between explanatory variables related to organizational practices and security compliance. Using quantitative approach and KHB analytical method as discussed in sub-sections 3.3.1 and 3.4.2 respectively, this chapter aims to examine the indirect effects of organizational practices on cyber security compliance. These indirect effects can then serve as a baseline for organisations to consider practices in place and also provide insights for cyber security research. In this thesis, three organisational practices will be investigated, *viz*., top management commitment, structured security processes and security investment.

The rest of the chapter is organised as follows. Section two discusses theoretical considerations used in this study. This is followed by variables measurement in section three. Section four and five assesses and discusses the research results respectively. Finally, section six finishes with the summary of this chapter.

5.2 Theoretical Considerations

This section aims to present an analytical framework that describes the effect of cooperation on organisational security practices towards cyber security compliance. Both public good and cooperation theories helped us in creating a novel framework taking into account fundamental security practices towards security compliance. This section presents variables required in constructing the analytical framework.

Following the arguments reviewed from the literature in chapter two, we formulate a research model that comprises key explanatory variables (organisational practices) namely, top management commitment (TMC), structured security processes (SSP) and security investment (SI) and a single mediating variable which is cooperation (COOP) to achieve cyber security compliance in organisations (See Figure 5.1). The purpose is to capture both the direct and indirect effects COOP have on these practices for employees to comply with security requirements as set forth in organisations.

TMC was studied due to its significance on security performance in organisations (Kankanhalli et al., 2003; Knapp et al., 2009; Knapp et al., 2006; Kritzinger & Von Solms, 2005; Kwon, Ulmer, & Wang, 2012) specifically its effect on compliance (Ahmed et al., 2012). In economics literature institutional role is critical to ensure the provision of public goods. This led to the decision to choose the next explanatory variable that is security investment. Investing on security technologies as well as competency has been associated with security compliance and heavily influenced by regulatory pressure (Cavusoglu et al., 2015; Moore, 2014). Without this pressure, security budget was seldom considered as top priority in organisations.

Previous studies discussed risk assessment and security incident response as main security processes in organisations, but these processes have been discussed separately. In this study, SSP was chosen considering the needs to combine both proactive (Järveläinen, 2013; Rocha Flores, Antonsen, & Ekstedt, 2014) and reactive (Ahmad, Hadgkiss, & Ruighaver, 2012; Line et al., 2008; Tøndel, Line, & Jaatun, 2014) approaches as a solid foundation in implementing security measures in organisations. Since there were limited studies that discussed the association of SSP with security compliance, we feel that it is important to investigate. This is because security processes provides a platform that requires actions to be collectively reached in meeting common security goals.

A manifest lack of cooperation by the employees of an organisation with the security efforts of the top management of the organisation has its roots in the former’s attitudinal indifference to these efforts. In these organisations, non-compliance may be said to stem from these employee behavioural indifferences to security. This is the direct effect of a lack cooperation on the part of the employees with the top management, middle management, technical teams and peers to prevent cyber security breaches. Such a behavioural attitudinal indifference of the employees towards security has great impacts on the organisation. Cyber security requirements such as security policies, standards, guidelines and best practices will only reach the user if the employees of the organisation will behaviourally cooperate with the top management in implementing the above measures to prevent cyber-security breaches. This is considered the indirect effect of cooperation. The indirect effect can also be observed through implementation of security processes that are structured in both proactive and reactive approaches. Interrelated tasks from various business units demand cooperative efforts through processes that are structurally designed for employees who will work collectively to meet security objectives. Similarly, when an organisation invest on security, cooperation between users and technology implementers is fundamental in ensuring that security breaches can be avoided.

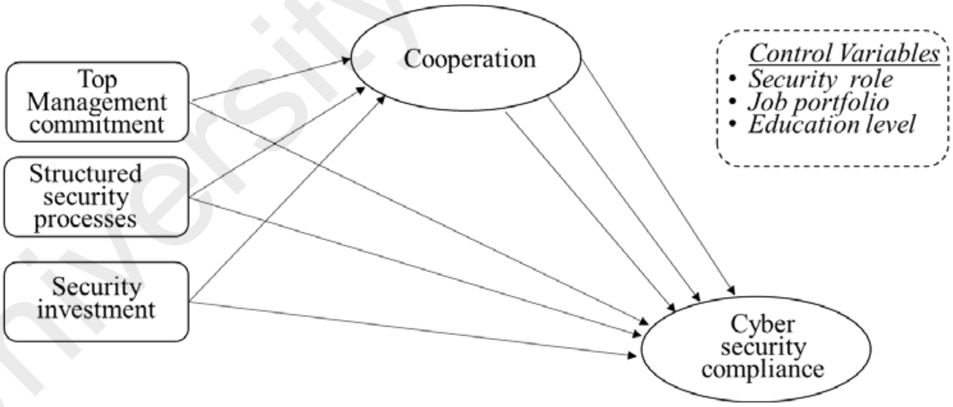


Figure 5.1: Analytical Framework of Organisational Practices and Cyber Security Compliance
Source: Author

5.2.1 Cyber Security Compliance

Cyber security compliance (CSC) is the dependent variable in our model. Whilst there was no solid evidence yet in associating CSC with cooperation at organisational level, Tyran and Feld (2006), posited that in the legal context neither rough sanction nor sanction-less compliance have been effective measures to achieve compliance. This suggests that non-deterrent sanction, such as self-imposed practices able to induce cooperation in complying with the law.

Referring to safety compliance from Griffin and Neal (2000) as core safety activities to be followed by employees at workplace, we define information security compliance as “a situation when employees in an organisation adhere with information security requirements in meeting information or cyber security objectives”. Adopting from Wood (1997), information security requirements can be channelled through policies and other related documents such as procedures, standards and legislations.

Previous security scholars drew on various theories such as deterrence theory, protection motivation theory, rational theory and planned behaviour theory to explain employees’ compliance behaviour. Those literature also pointed to various factors that contribute towards information security compliance in organisations. According to Safa, Von Solms, and Furnell (2016), information security knowledge sharing, collaboration, intervention and experience have a significant effect on employees’ attitude towards compliance with organizational information security policies. Puhakainen and Siponen (2010), argued that continuous communication processes are required to improve users’ policy compliance while information security training needs to adopt methods that motivate learners to adopt systematic cognitive processing of information received during training.

Goo, Yim, and Kim (2014), suggested for information security climate as an alternative to a sanction-based deterrence in policy compliance. So that an employee's affective and cognitive states are nurtured through affective and normative commitment. Meanwhile, Ifinedo (2014), acknowledged how social bonds formed at work and subjective norms could positively affect employees’ information security policies compliance. Bulgurcu, Cavusoglu, and Benbasat (2010), posited that employees’ intention to comply with information security policies is significantly influenced by attitude, normative beliefs, and self-efficacy to comply, which corroborated by Ifinedo's (2012) finding that self-efficacy, attitude toward compliance, subjective norms, response efficacy and perceived vulnerability could positively influence information security behavioural compliance. According to Vance, Siponen, and Pahnila (2012), habit (a routinized form of past behaviour) influences threat appraisals (vulnerability, perceived severity and reward) and coping appraisals (response efficacy, self-efficacy and response cost) that affect employees intention to comply with cyber security policies.

Non-compliance with regulatory requirement can implicate not only the reputation and revenue of organisations, but can also attract penalties (Basu, 2014). However, being compliant with regulatory requirements does not indicate good security posture of any organisation (Basu, 2014; Mohammed, Mariani, & Mohammed, 2015; Valentine, 2010). Valentine (2010), argued that organisations become vulnerable when they are too complacent and lack of monitoring. In referring to mandatory compliance with Payment Card Industry Data Security (PCI-DSS) standards for handling credit cards in the US, Valentine (2010), asserted that organisations have the mind-set, where upon complying with this standard, they feel secure that they will avoid future security breaches. What most organisations have overlooked is the fact that although the payment related systems are compliant, other aspects or controls connected to these systems may be violated.

5.2.2 Cooperation

Cooperation (COOP) is the mediating variable used in this thesis which is important as the underlying factor to achieve security compliance in organisations. Although there were no previous studies that associate cooperation with security compliance in organisations, participation in organisational security initiatives could be regarded as a proxy for cooperation (Hu et al., 2012; Vroom & Von Solms, 2004). These studies demonstrated the influence of participation by top management in shaping employees' attitudes to comply with security policies. Cooperation that cut across departmental units is fundamental for critical business functions to work cohesively to accomplish organisational objectives. As revealed by Rodríguez, Pérez, and Gutiérrez (2008), cooperation has been identified as a significant contributor to the success of new product development. Meanwhile, findings of a study on checking the presence of cooperation between staff of ICT and power automation units disclosed a lack of cooperation of these units in performing operational tasks (Line, 2013). The needs for a closer cooperation between them not only can improve operational performance, but ensure that the integrated systems are workable and reliable in both peace and crisis time. In general context of public goods, Kaul, Grungberg, and Stern (1999) stressed the importance of cooperation as an additional mechanism in ensuring that public goods to be adequately provided. However, the cooperation they referred to was not related to cooperation within organisations, but cooperation at the global level.

5.2.3 Top Management Commitment

Managing by commitment is characterized as underlying practices of management in crafting strategies, executing them and also leadership style (Sull, 2003). Top management commitment (TMC) refers to how senior management groups lead and guide employees towards organisational performance (Teh, Ooi, & Yong, 2008). They influence the others in meeting organisational objectives and outcome (De Jong & Den Hartog, 2007) through practicing what were defined in organisational policies. Through management commitment, resources allocation and support will be facilitated in ensuring successful projects in organisations (González & Guillen, 2002). Previous security scholars also asserted the importance of TMC in the forms of support (Knapp et al., 2009; Knapp et al., 2006) as well as financial resources (Azizan Ramli, Mazlin Mokhtar, & Badhrulhisham Abdul Aziz, 2014).

Jacqueline, Shahram, and Thomas (2011), demonstrated that organizations which their top management put high commitment in security efforts engaged more in preventive security initiatives than those with lesser support. Without their support and involvement, security initiatives and efforts will not be effectively implemented (Knapp et al., 2006; Kritzinger & Von Solms, 2005). TMC which is an attribute of information security governance in organisations (Von Solms, 2005) could ascertain for organisational objectives to be achieved (Azizan Ramli, Mazlin Mokhtar, & Badhrulhisham Abdul Aziz, 2014; International Organization for Standardization, 2013). The top management should also encourage cooperation between those who have supervisory roles and their subordinates in performing daily tasks particularly that involved sensitive information. Musa (2012, p. 104) contended that an absence of cooperation between these two levels of employees could create problem and increase risk in organisations. Although top management is responsible in providing technological resources as part of internal security control, this should not be left to the technical teams alone. The management together with their senior and junior managers should review the effectiveness of the security controls implemented (Musa, 2012, p. 105). Not only to ensure organisational security goals are achieved, but the security governance is met. Having security measures in place without enforcement from the top management cannot ensure that compliance is met. It is the top management that is responsible to ensure the deployment of relevant security mechanisms e.g. security policies, procedures and standards follow the organisational directives and enforced accordingly (Musa, 2012, p. 52). However, the reluctance of top management to abide by security efforts, give different signals of their commitment level and support, eventually demotivate their employees to comply (Puhakainen & Siponen, 2010).

5.2.4 Structured Security Processes and Tasks Interdependence

One big challenge in protecting organisations from successful cyber attacks is when employees need to work on all aspects of defending their organisations, but attackers only focus on a certain point of vulnerability. Business processes should be structured and continuously improved. This is to understand strategies used by cyber attackers and also cyber threats due to change of technologies (Batra, 2010; McGourty, 1998). Using discipline approach in software development, Batra (2010) recommended for relevant processes to be structured, standardised and documented. This is to allow those who are non-experts to benefit from these processes thus, leads to conformity of such processes.

In ensuring confidentiality, integrity and availability of information be protected and secure when it goes across a network (Posthumus & Von Solms, 2004), security processes need to be structured in managing security in proactive and reactive manner. Proactive process is to detect and prevent security breaches from occurring while reactive allows for breaches to be responded to in a quick and effective manner (Baskerville, Spagnoletti, & Kim, 2014; Juhee & Johnson, 2014) where these two processes do not operate in isolation (Baskerville, Spagnoletti, & Kim, 2014). Thus, we argue that these processes cannot be isolated due to tasks interdependence that exist among business units in organisations. Wageman (1995), asserted that high interdependence task can promote cooperation. The higher task interdependence exist in groups the more importance of information sharing and other cooperative behaviours needed to complete those tasks (Thomas, 1957).

According to McGourty (1998), in engineering line, structured processes is the foundation for continuous improvement apart from strong assessment where both provides a roadmap for employees. Throughout the design and implementation process, participation is required from all across the organisation using this roadmap for them to follow (McGourty, 1998).

Similarly, in the context of information security, structured processes are extremely necessary as they require participation among employees to prevent security breach. In this study proactive processes that are being discussed are ISMS and BCM[8], while the reactive processes are security incident management procedure that also includes digital evidence management[9]. Within these processes, there are interrelated tasks that demand cooperation to ensure security measures are communicated and implemented effectively.

There were two main contributions from task interdependence efforts that signify how cooperation level can be affected through social interaction in group: firstly, more communications and information sharing in the groups and secondly, through group rewards (Wageman, 1995). Guzzo and Shea (1992) in view that for task interdependence to present there should be some degree of interactions and coordination among group members in completing their tasks in which that mutual dependence is formed when the degree of interdependence is high (Ramamoorthy & Flood, 2004). The significance of having mutual dependence is that the goals of individualists and groups can be closely aligned (Ramamoorthy & Flood, 2004) as they are implementing tasks in meeting a common goal. As suggested by Ramamoorthy and Flood (2004), in an environment where task interdependence is high, individualists tend to move away from their own objectives, but closer to the group by being helpful and cooperative. In a complex operating environment where there are high interdependencies within groups in the

[8] ISMS and BCM are discussed in details in sub-section 2.3.9.1
[9] Security incident management procedure and digital evidence are discussed in 2.3.9.2

organisation itself and inter-organisations, it is more than often that consistent and high level of interactions are required (Wageman, 1995).

In providing this type of interaction, security processes should be structured, documented and disseminated to allow employees to perform their tasks in according to the structured security processes. Based on an empirical investigation conducted by Rocha Flores, Antonsen, and Ekstedt (2014), their results suggested that a process should be established to coordinate security activities as a mechanism to increase security knowledge of employees. This can be materialised in organisations as one of security controls in handling human errors pertaining to information security.

According to Kolkowska and Dhillon (2013), failing to create understanding of new security processes and security requirements to users lead to failure in changing their behavioural intention to follow the requirements. In responding to cyber security breaches, two phases of security processes are worth considered for implementation; proactive and reactive practices. In proactive phase, organisations deploy processes that able to identify security threats, vulnerabilities, minimize impacts to organisations if cyber security breaches were to occur. Being proactive, organisations able to demonstrate capabilities to foresee impending cyber threats and develop initiatives to prevent cyber security incidents from happening. Thus, organisations are able to strengthen their security measures by continuously improving security benchmarking in components (Pye & Warren, 2005). Even if they were to occur, counter measures could have been in place to minimize the impacts. Three major critical proactive measures discussed are information security risk assessment, security vulnerability assessment and business continuity management.

While being proactive, it is also critical for organisations to quickly react to security breaches by implementing response procedures. Two reactive measures that are significant for deployment are cyber security incident management and digital collection and preservation procedures in place. The earlier is mainly deployed to contain security incidents from spreading and recover from the incident the soonest possible while the latter is to ensure digital evidence is acquired correctly and acceptable for investigation purposes. It is also important in this phase to identify the root cause of the breaches and learn from lessons of the incident for improvement.

Both phases require cooperation to collectively adhere to security processes in performing tasks that are required for business operation. There are some form of integrations needed between these processes that could affect the magnitude of security breaches once occur.

Using a strategic roadmap, McGourty (1998) contended that structured processes as a tool to assess engineering process in organisations. McGourty (1998), further reasoned that structured processes were the foundation of organisation's continual improvement which required participation throughout the organisation in designing and implementing the processes. In the context of information security, Juhee and Johnson (2014), suggested that improvement of information security processes demand continual learning of strategies used by attackers and also emerging technologies that consistently introduce new security threats. Thus, adapting both proactive and reactive intervention is necessary (Juhee & Johnson, 2014).

Previous scholars considered that the implementation of Information Security Management Standard (ISMS), which is expounded by the risk-based security management approach based on ISO/IEC 27001 can cut as a tool in managing security. This international standard requires structured security processes and ISMS itself has been particularly renowned for being a significant proactive process implemented to reduce security risks and threats related to information assets (Dey, 2007; Zahri Yunos et al., 2014). One distinct feature ISMS is the needs to have a process in checking security compliance (International Organization for Standardization, 2013). Another proactive process that is worthy to implement is business continuity management which is able to assure continuous availability of services and data in organisations.

Depending on security efforts initiated by countries in protecting their cyber space, role of institutions in setting requirements relevant to security processes should not be underestimated. Requirements set by the Federal Information Security Management Act (FISMA), (a piece of United States legislation that defines a framework to protect government information for organisations to assess security position) indicate the needs for security assessment to be conducted periodically to identify areas for improvement (Mohammed, Mariani, & Mohammed, 2015). Having periodic security assessment include assessing vulnerabilities at different levels such systems, devices, application and databases is crucial to detect vulnerabilities that could cause security breaches. Previous security scholars also claimed that undetected security vulnerabilities or weaknesses in software and systems contribute to cyber security breaches (Anderson, 2001; Anderson & Moore, 2006; Permann & Rohde, 2005; Schneier, 2007). Schneier (2007), suggested for softwares to be tested to avoid insecure software due to poor design. Without proper testing and assessment, security vulnerabilities could not be identified, thus leading to easy exploitation. Similarly, a directive was issued by the Malaysian cabinet that requires organisations in the critical sectors to implement ISMS and obtain certification (CyberSecurity Malaysia, 2011). ISMS is a holistic approach to manage cyber security from the lens of risk management. Suhazimah Dzazali and Ali Hussein Zolait (2012), asserted the needs for risks to be managed in organisations due to fast technology changes and increase of cyber attacks.

Responding to security incidents and analysing data after the breach is a critical reactive process (International Organization for Standardization, 2011; Line, 2013). Line (2013), asserted a lack of systematic approach to respond to cyber security incidents in control system environment and how incident management is mainly based on tacit knowledge through experiences of users. This can be a serious issue as Line et al. (2008) found that the respondents have not experienced serious security incidents that could test their response capability where failure of this could give huge impact to their organisations. Cyber security professionals and practitioners agree that having the capabilities in handling cyber security incidents is fundamental to minimize the adverse effects of security breaches have on organisations. The root cause of security incidents need to be investigated immediately after the breach for remedial purposes (Baskerville, Spagnoletti, & Kim, 2014; Mohammed, Mariani, & Mohammed, 2015).   Mohammed, Mariani, and Mohammed (2015), further suggested for information on cyber security incidents in healthcare sector to be shared within the sector in order to strengthen the overall incident responses in the sector. Delay in identifying causes of an incident can delay in providing remedial actions.

Both security processes comprise interrelated tasks that demand cooperation at all levels to ensure implemented security measures are effective and meeting security objectives. In performing tasks within these processes, some form of integration is needed in these processes in minimizing the magnitude of security breaches.

5.2.5 Security Investment

As organisations are pressured to comply with regulatory requirements, the level of investments were anticipated to increase to prevent security breach (Cavusoglu et al., 2015).   In building organisational security capabilities, investment should not only focus on technologies, but also the non-technology aspects (Bonderud, 2016; Swarts, 2015).

Bonderud (2016), argued that for organisations to invest only on technology in building security defence is not sufficient. Instead, Bonderud (2016) put forward the needs of organisations in becoming active security players by embedding people aspect in the process. In other words, having people being an integral part of the process explains the needs of relevant skillsets, experiences and competencies to understand and make full sense of security technologies. Employees' capabilities and competence related to information security have a positive effect on compliance behavioural intentions (Ifinedo, 2014).

For successful technologies deployment, cooperative efforts are necessary among systems owners, system implementers and users. Lack of formal components for technical implementations such as trainings and manuals may cause reluctance of employees to implement and perform such technical deployment (Musa, 2012). In a different context, technical components of security systems need users' cooperation in providing a more secure and efficient state of organisational security (Arduin & Vieru, 2017). In situations where organisations have security outsourcing arrangement with external parties, Mulej, Rebernik, and Bradac (2006), asserted the needs for cooperation to ensure its success. Not only cooperation between outsourcer and outsourcing provider is paramount to ensure compliance, but also between management, systems and processes. Interestingly, they further argued that limitation of human mental capabilities demands cooperation and without it, individuals are not capable to solve complex problems.

Security investment made by organisations were mainly on technologies and equipment that were to be deployed to protect computer systems and network perimeter. However, having solely technologies in place are not enough. Technologies deployment require human intervention that have relevant skills and expertise in manning them. Thus, these security experts need to cooperate not only with other technologies owners such as other departments or branches (if the systems are decentralised), but also with the external technologies' providers such as outsourcing. In situations where organisations have outsourcing arrangement with external parties, cooperation is fundamental since it involves trust and cooperation. For outsourcing relationship to succeed, cooperation between outsourcer and outsourcing provider is paramount. Since outsourcing arrangement is built on trust, equal information sharing by both parties is significant for mutual benefits of both parties. In a situation where information asymmetry exists, one party may lead to opportunistic behaviour that would eventually leads to the failure of the relationship.

5.3 Variable Measurements

To operationalise the constructs in answering research question 2, we adapted some items from previous relevant studies as discussed below. We also developed new constructs that were not published before. There are five variables used to answer the second research question. We measured CSC by assessing the likelihood of respondents' organisations of achieving cyber security compliance with the present of cooperation in organisations. See Appendix A section 2. In the survey, information about cyber security compliance was obtained and coded in a five-point Likert scale namely, 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree and 5 = strongly agree. In providing clarity of responses of the dependent variable, relevant scale items were collapsed into three categories; where (i) responses on strongly disagree and disagree were combined and coded as 1 = disagree, (ii) neutral responses remained as 2 = neutral and (iii) agree and strongly agree responses were combined and coded as 3 = agree. Meanwhile, constructs of TMC, SSP and SI were measured as continuous variables and established by summing and averaging the respective scale items.

TMC was measured based on commitment demonstrated by top management in information and cyber security (TMC1) and enforcement of security policies, procedures and other requirements in organisations (TMC2). For this construct, respondents were asked to indicate the commitment shown by their top management. See Appendix A section 2. We adopted this measure that was manifested in various forms; policy formulation and enforcement effectiveness (Knapp et al., 2009; Kwon, Ulmer, & Wang, 2012) and top management participation in security programmes (Hu et al., 2012).

With respect to SSP, this construct referred to proactive (SSP1) and reactive security (SSP2) processes that were implemented to protect information through involvement and cooperation amongst employees in organisations. See Appendix A section 2. Adopting previous research on both approaches (Baskerville, Spagnoletti, & Kim, 2014; Juhee & Johnson, 2014), proactive process focused on risk (Suhazimah Dzazali & Ali Hussein Zolait, 2012; Zahri Yunos et al., 2014), vulnerabilities and data recovery and continuity (Aronis & Stratopoulos, 2016; Järveläinen, 2013; Johnson, 2014) whereby reactive process emphasizes the aspect of incident response and management (Ahmad, Hadgkiss, & Ruighaver, 2012; He, Johnson, & Lu, 2015). The final explanatory variable, SI, referred to investment on security technologies (SI1) and technical capabilities and practice (SI2, SI3 and SI4). See Appendix A section 2. This variable was adapted from previous works that have been identified as pertinent to this study (Ifinedo, 2012; Mulej, Rebernik, & Bradac, 2006; Swarts, 2015). Technologies deployment require human intervention through skills and expertise in manning them. Employees have the tendency to follow security policies when they have relevant skills and competence in implementing security measures (Ifinedo, 2012).

In this study, cooperation served as a variable that had the mediating effect between TMC, SSP and SI and CSC. Established as a single item variable, it captured the level of cooperation observed in organisations. Adopting the output of a study conducted by Rodríguez, Pérez, and Gutiérrez (2008), cooperation was identified as a contributing factor to organisational performance. Cooperative behaviour among employees in complying with security requirements could minimize opportunistic behaviour in organisations.

In addition to the three explanatory variables above, we also controlled using three control variables namely, security role, job portfolio and educational level. In order to test the mediation effect of the relationship of the selected practices with CSC, it is necessary to consider these variables. Although Williams (2008) and Wylder (2003) argued that everyone was responsible to ensure information was protected and secure in organisations, there were groups of employees that were provided with roles and responsibilities to meet organisational security objectives e.g. top management, middle management and technical operations. While top management were to provide resources and commitment, middle management was observed to serve other levels such as top management, technical team and end users. Measurement of security role is discussed in sub-section 4.3.2. Job portfolio is based on demographic data that has five categories that were later collapsed into three categories. The first category comprised those who directly involved with ICT security and responsible to ensure the overall security was taken care of including systems, applications and physical. Next, groups were those who were indirectly related with security including ICT operations and ICT planning, ICT risks and other related tasks. The final control variable was educational level which was grouped into three categories of highest education; bachelor, masters and phd.

5.4 Results

In answering the second research question, the analysis is divided into two types; descriptive and statistical analysis. Descriptive analysis is discussed in sub-section 5.4.1 while statistical analysis using the KHB method is discussed in sub-section 5.4.2.

5.4.1 Descriptive Analysis

Sample demographic characteristics are deliberated in sub-section 4.4.2. As for data normality, Jarque-Bera test was performed prior to determination of the analytical method. Data normality is discussed in sub-section 4.4.4. Missing data was later assessed where less than 10 % missing data was detected in random fashion which is acceptable (Hair et al., 2010).

In testing the internal consistency of the variables, Cronbach value was computed where the results show that the computed values were 0.6 and above. The Cronbach coefficient alpha values for measuring TMC (0.78), SSP (0.63) and SI (0.66) are indicated as acceptable reliability values (Moss et al., 1998). Cronbach's alpha internal consistency reliability value of 0.7 or higher is considered acceptable (Gliem & Gliem, 2003; Nunnally, 1978). However, Suhr and Shay (2009) suggested that 0.6 was acceptable if the analysis was for research purposes. Several researchers had since used the 0.6 value (Setbon & Raude, 2010; Waljee et al., 2010). Another study had argued cogently that alpha values lower than 0.6 was insufficient while higher than 0.8 suggested redundancy in measuring the construct (Streiner & Norman, 1989).

The descriptive statistics of the variables used in this study are exhibited in Table 5.1 where statistics specific to TMC, SSP and SI and CSC are presented.

Table 5.1: Descriptive Statistics of the Variables Used for KHB Analysis

	n, (%)	**Mean, (SD)**	**Disagree (n, %)**	**Neutral (n, %)**	**Agree (n, %)**
Cyber security compliance[a]	155, (100)	2.63, (0.624)	12, (7.74)	33, (21.29)	110, (70.96%)
Top management commitment[b]	155, (100)	3.58, (1.19)	-	-	-
Structured security practices[b]	155, (100)	3.90, (0.53)	-	-	-
Security investment[b]	155, (100)	3.48, (0.63)	-	-	-
Cooperation	155, (100)		-	-	-
Cooperation=1	139, (89.68)	-	5, (41.67)	26, (78.79)	108, (98.18)
No cooperation=0	16, (10.32)	-	7, (58.33)	7, (21.21)	2, (1.82)
Job Portfolio					
ICT operation	43, (27.7)	-	4, (33.33)	12,(36.36)	27, (24.55)
ICT security	76, (49.1)	-	4, (33.33)	9, (27.28)	63, (57.27)
Other ICT functions	36, (23.2)		4, (33.33)	12,(36.36)	20, (18.18)
Security role					
Top management	23, (14.84)	-	2, (16.67)	6, (18.19)	15, (13.64)
Middle management	80, (51.61)	-	6, (50.00)	16, (48.48)	58, (52.73)
Technical management	52, (33.55)	-	4, (33.33)	11, (33.33)	37, (33.63)
Educational level					
Bachelor and Diploma	93, (60.00)	-	7, (58.33)	20, (60.61)	66, (60.00)
Masters	43, (27.75)	-	2, (16.67)	11, (33.33)	30, (27.27)
Phd and above	19, (12.25)	-	3, (25.00)	2, (6.06)	14, (12.73)

Note:
n- total observations, SD=Standard Deviation
[a] Dependent variable was measured by Likert scale which was later collapsed into 3 categories: Disagree, Neutral and Agree
[b] These independent variables are measured by the Likert scale (from 1=strongly disagree to 5=strongly agree)
Source: Computed from Author's Survey

We summarised the findings as follows. Firstly, 70.9% respondents reported that they agreed that CSC was achieved in their organisations followed by disagree category at 7.7% and neither of both categories at 21.3%. Secondly, in relation to agreeing that CSC was achieved in their organisation, 98.2% of respondents indicated that a high cooperation level contributed to the compliance. Finally, the average response of all the explanatory variables with standard deviation varied: for example TMC (mean=3.58, SD=1.19), SSP (mean=3.90, SD=0.53) and SI (mean=3.48, SD=0.63). These results show that respondents agreed SSP was highly practiced in their organisations in comparison to TMC and SI. These findings could be influenced by the implementation of ISMS pursuant to the Malaysian Cabinet Directive issued in 2009.

In detecting multi-collinearity problem, the models were later tested using Variance Inflation Factor (VIF) where estimates of the VIF fell between 1.00 to 1.90 for all items. According to Marquaridt (1970) variance inflation factor was acceptable in the range of 1.0 to 10 confirming that there was no multi-collinearity issue in the overall model.

5.4.2 Mediation Statistical Analysis

Table 5.2 presents the mediation analysis results by the type of organisational practices after controlling for security responsibility level, job portfolio and educational level. Four major findings were observed. Firstly, all independent variables have direct associations with CSC, TMC (OR = 3.030, p = 0.000), SSP (OR = 2.716, p = 0.009) and SI (OR = 2.961, p = 0.002). Secondly, the inclusion of cooperation significantly reduced the direct effects of the two organisational security practices: TMC and SSP on CSC. The magnitude of the total effect of security practices when top management involved in security efforts was 1.330 (odds ratio (OR) =3.782) when cooperation was introduced with the co-efficient of TMC was statistically significant at 1% significance level and positive. This indicates that for every unit increase in TMC, the expected ordered log odds increased by 1.330 as CSC moved to the next higher category (that is from disagree to neutral category and from neutral to agree category) in achieving CSC, given all of other variables in the model were held constant. However, the magnitude of direct effect was reduced to 1.108 with OR=3.030 when cooperation was included in the relationship.

The difference of the magnitude of 0.221 (indirect effect) represented the mediating impact that was statistically significant at 1% significance level and positive.

Similarly, there is also a positive mediating effect between SSP with CSC which is significant at 1% significance level. For every unit increase in SSP, the expected ordered log odds increased by 1.440 as CSC moved to its next higher category. As cooperation mediating the relationship, the effect of SSP reduced to 0.999, leaving an indirect effect of 0.441. However, the decomposition results show that the mediating effect on CSC by SI was not significant suggesting that no mediation effect took place. However, it is worthy to note that there is a positive direct effect of this relationship which is significant at 1% significance level.

The importance of cooperation is profound in both TMC and SSP. The overall results show that the inclusion of the cooperation reduced the magnitude of effects between TMC and SSP with CSC, but not SI. The KHB test calculated indirect effect of TMC and SSP at p = 0.221 and p = 0.441 respectively in the relationship after cooperation was included to the model, confirming cooperation as the mediator. The direct effect for both TMC and SSP remained significant after mediation indicating that partial mediation had taken place with the percent of mediation (ratio of the indirect effect to total effect) is P_M = 16.17 and P_M = 30.63 respectively. The results of this study are supported by Scott, Bishop, and Chen (2003) where tasks interdependence are positively related to willingness to cooperate.

Cooperation that requires collective action to perform integrated tasks across organisations is proven to be significant to achieve CSC. These findings are supported by De Cremer and Van Knippenberg (2002) where cooperative interactions were necessary when task interdependence involved. These findings are also supported by

Suhazimah Dzazali and Ali Hussein Zolait (2012) where security processes and risk management were crucial to understand the landscape of security in the government sector in Malaysia. Following the anonymous attack in year 2012, apart from security processes, skilled manpower was also identified as measures to effectively deal with cyber attacks in organisations (Bernama, 2011). The role of institution has also been found to be effective where there has been an increase in number of organisations obtained ISMS certification in Malaysia from 62 in 2010 (*ISO/IEC27001*, n.d.) to 262 in 2017 (Department of Standards Malaysia, 2017). The increase also demonstrates mimetic

Table 5.2: The KHB Mediation Analysis by Organisational Practices and Cyber Security Compliance

Characteristic	**Coefficient,β**	**Standard error (SE)**	**95% Confidence Interval**		**Odds Ratio (OR)**
			Lower bound	**Upper bound**	
Top Management Commitment (TMC)					
Total effect	1.330***	0.218	0.902	1.758	3.782
Direct effect	1.108***	0.216	0.685	1.531	3.030
Indirect effect	0.221***	0.073	0.078	0.365	1.248
P_M (% of mediation)[a]	16.66%				
P_M (% of mediation)[b]	15.62%				
Structured Security Practices (SSP)					
Total effect	1.440***	0.378	0.698	2.182	4.223
Direct effect	0.999***	0.380	0.253	1.745	2.716
Indirect effect	0.441***	0.161	0.126	0.756	1.554
P_M (% of mediation)[c]	30.63%				
P_M (% of mediation)[d]	27.23%				
Security Investment (SI)[e]					
Total effect	1.294***	0.357	0.592	1.996	3.648
Direct effect	1.085***	0.352	0.395	1.775	2.961
Indirect effect	0.208	0.135	-0.056	0.473	1.231

Notes:

1. All the control variables were included in the analysis and only the mediation results were reported
2. [a] Mediation effect with control variables (security role, educational level)
3. [c] Mediation effect with control variables (educational level, job portfolio)
4. [b,d] Percentage of mediation without control variables
5. [e] Control variables for this association (security role, educational level, job portfolio)
6. *** - significant at 1% significance level

Source: Computed from Author's Survey

isomorphism where other organisations follow the adoption of ISMS in CNII sectors in becoming risk averse organisations.

Secondly, there was an effect of control variables in controlling the relationship. The results show a slight increase of mediation effect on TMC by 1% controlling by both educational and responsibility levels, where cooperation was likely influenced by the intervention of top management and implementation efforts by the middle management. Meanwhile, the effect is higher on SSP by 3.4% controlling by educational level and job portfolio. This was mainly due to the fact that almost half of the respondents (49.1%) held ICT security portfolio who were directly responsible for performing security tasks and for ensuring security measures were in place. These findings were supported by ISACA (2012) where processes should be defined and communicated, particularly security process (Suhazimah Dzazali & Ali Hussein Zolait, 2012).

Thirdly, in this model SI was significant in predicting CSC to be achieved in CNII organisations. However, it was not significant if CSC were to be achieved through cooperative efforts such as cooperation between people’s technical competence (refers to professional skills) and security technologies required to implement security measures. Simply put, the biomass of professionally trained cyber security professionals is inadequate to address the current cyber security threats as described in this thesis. This could be explained by limitations of those who had professional certifications which is only at 39.7%.

5.5 Discussion

The section begins with the discussion of cooperation in achieving cyber security compliance. This is followed by the sub-sections that discuss the mediating effects of the three significant cyber security practices on cyber security compliance.

The results of this study suggest that cooperation as the mediating factor stimulates employees to comply with organisational security requirements in which cooperative efforts are embedded in organisational practices such as TMC and SSP. Contrary to previous studies where fear factor, threat appraisal, social bond and sanctions influence security compliance, this study provides evidence that collective actions by employees through cooperation contribute to compliance.

The findings of this study are also supported by Veiga and Eloff (2007) where cooperation among employees throughout the process of changing behaviour while establishing security processes is paramount. The cooperative behaviour in groups can be further promoted through stimulation of communications and information sharing (Wageman, 1995). Rocha Flores, Antonsen, and Ekstedt (2014), supported this further that efforts in managing information security can be coordinated through relevant security processes that include information security risk assessment, security controls implementation and effective monitoring of selected controls; which can be realised through ISMS implementation. ISMS that demands continual improvement to strengthen security measures in organisations (Pye & Warren, 2005) demonstrated its capabilities in reducing information risks and threats in organisation (Dey, 2007).

In the context of business continuity planning, cooperation among business units is fundamental that involves critical tasks such as identifying critical business functions and exercising those functions (Holowachuk, 2007). The former requires identification of resources, information and interdependencies among them while the latter emphasizes exercising procedures to ensure critical services are available in the event of disaster. Thus, the results of this study are supported by Aronis and Stratopoulos (2016) where cooperation is crucial for IT department to work with other business units to rehearse recovery procedures in preparation for disasters viz., cyberattacks. It is critical to ensure that business function owners are familiar regarding actions to be taken in the event of disasters as documented in their continuity plans and procedures. These exercises are performed in routine where cooperation is profound at all levels in organisations. The author submits that exercising business and security procedures promote cooperation in organisation. This is because there is a familiarisation of roles and lessons to be learnt from the rehearsals. This is supported by Nelson and Winter (2002) who posit that learning from routine and skills and practicing those for perfection can promote behavioural continuity.

Both proactive and reactive processes above clearly show the existence of task interdependence that calls for employees to cooperate. This is in line with Guzzo and Shea (1992), who asserted that for task interdependence to be present, there should be some degree of interaction and coordination among the group members to complete their tasks which can be found in those processes. According to Ramamoorthy and Flood (2004), when the degree of interdependence is high, a mutual dependence is formed that can influence individualists (who is more concerned in fulfilling own obligations) and those who are in the group to work collectively towards common goals as they perform their tasks.

5.5.1 Cooperation and Achieving Cyber Security Compliance

CSC cannot be achieved either by organisations or employees alone; it requires cooperation; internal and external. Cooperation is established through commitment demonstrated by top management and implementation of security efforts through structured security processes. Cooperation in organisations can be induced by TMC through a sense of belongingness instilled in all employees by diverting individual interests to become more collective in working towards a common goal.

As deliberated in sub-section 2.3.6.1, compliant behaviour can be triggered by various factors depending on circumstances. When people are treated fairly and procedural justice is observed, their tendency to cooperate in compliance is greater (Murphy, Tyler, & Curtis, 2009). People also tend to comply when they get assistance that is cooperation from authorities, to reduce complexities. As argued by Langham, Paulsen, and Härtel (2012) in tax filing practice in Australia, taxpayers expected for cooperation from the tax office to help them fill the tax form to enable them to submit tax form as required by the law.

Cooperation takes different forms; through management commitment, structured security processes and security investments. Through management commitment, cooperation is induced when management provides budget and resources for implementing security requirements. In addition, necessary enforcement on policies and procedures should also take place. Cooperation is also extended to employees when top management such as Chief Executive Officers (CEOs) are present and participate in organisation's related security programmes such as cyber drills or business continuity exercises. The author submits that cooperation in organisation can also be achieved through awareness of security programmes, effective communication of these programmes and social bonds created by middle management in implementing security efforts that bridge top management intent with employees. Thus, cooperative efforts are able to drive compliance.

As argued by Tyler and Fagan (2008), cooperation can be obtained from the public in complying with the law, in this context where public is required to report crimes to the authorities. However it is conditional. They will only cooperate to comply when they know that they are reporting to a legitimate party that is the police. Similarly, in the context of SSP, employees cooperate in reporting security breaches when they know that there is an established process for them to do the reporting. Thus, getting them to cooperate in understanding when and how to report the incidents efficiently, awareness is not sufficient. It requires a structured incident management procedure to be developed and exercised, get relevant employees to understand the procedure and how to react in accordance with the procedure. Complying with security procedures is as crucial as complying with security policies as the latter provide high level direction for employees to follow the rules set in the policies. To support the security policies, procedures are needed in order for employees to understand on how to do it on a step-by-step basis.

5.5.2 Top Management Commitment and Cyber Security Compliance

Previous studies have shown the impact of top management on employees' behaviour in complying with security requirements in organisations (Hu et al., 2012; Knapp et al., 2009; Knapp et al., 2006; Kwon, Ulmer, & Wang, 2012; Puhakainen & Siponen, 2010). However, this study demonstrates that cooperation induced by senior management through instillation of a sense of belongingness among employees can divert individual interests into more collective interests in working towards common goals. This is supported by Mulder, van Dijk, and De Cremer (2009), where the likelihood for compliance to increase is largely dependent on how convincing the leaders are in encouraging cooperation especially in situations where sanctions were clear in place. This can be resulted from high trust level on leadership in organisations (Mulder, van Dijk, & De Cremer, 2009). Since trust has been central to information security studies (Flowerday & Von Solms, 2006; Veiga & Eloff, 2007) and cooperation (Jeffries & Becker, 2008; Smith, Carroll, & Ashford, 1995), building a trusting relationship between management and employees is important.

Empirical evidence has shown that top management has a significant impact on employees compliance behaviour (Hu et al., 2012) that contributes to security compliance in organisations (Hu et al., 2012; Puhakainen & Siponen, 2010). TMC is demonstrated through adequate resources, budget allocation and support in ensuring organisational objectives are achieved (Azizan Ramli, Mazlin Mokhtar, & Badhrulhisham Abdul Aziz, 2014). In addition, top management commitment is reflected through its seriousness in handling information security by assuring that security policies and procedures are enforced and adhered to. Having top management commitment capable to provide the right directions of cyber security aspects in aligning with organisational objectives, which is also attributed to information security governance in organisations (Von Solms, 2005). Leadership and top management commitment in information security in organisations has been clearly demonstrated as one of requirements in complying with ISMS (International Organization for Standardization, 2013).

Cooperation is also demonstrated to employees when top management such as CEOs were present and participate in the implementation of security programmes in their organisation. Top management participation in information security programmes in complying with security policies (Hu et al., 2012) indicate their cooperative efforts in motivating employees to work together in meeting common security objectives. Apart from participation, top management reflects their commitment not only through provision of budget and resources (Azizan Ramli, Mazlin Mokhtar, & Badhrulhisham Abdul Aziz, 2014), but ensure enforcement of relevant security policies and procedures (Knapp et al., 2009; Kwon, Ulmer, & Wang, 2012).

TMC can also determine the success of projects in organisations (Azizan Ramli, Mazlin Mokhtar, & Badhrulhisham Abdul Aziz, 2014; Chan Wai Kuen, Suhaiza Zailani, & Yudi Fernando, 2009) and the overall effectiveness of information security aspects in organisations (Hawkey, Muldner, & Beznosov, 2008). In related to the latter, Proviti (2016), posits that engagement of board members in organisational information security risks leads to effective security measures in organisations.

5.5.3 Structured Security Processes and Cyber Security Compliance

Results of this study show that structured security processes is significant in contributing to cyber security compliance in organisations. The results are also supported by Rocha Flores, Antonsen, and Ekstedt (2014) on the needs for organisational processes to be formally documented and communicated in organisations, so that information security knowledge could be shared in organisations. Although their studies did not indicate achieving security compliance as the utmost outcome of these processes, their findings are significant to support this study.

As deliberated earlier, proactive processes are processes are established in preparing organisations to prevent, defend and plan to recover from security breaches while reactive processes are designed for organisations to react, respond and recover from security breaches. The next sub-sections discuss proactive process including information security risk assessment, security vulnerabilities and business continuity management while reactive discusses incident management. The following section discusses these structured processes and how cooperative efforts are embedded in them to ensure achieving CSC in organisations.

5.5.3.1 Information Security Risk Assessment

In order to understand cyber security posture in organisations and plan for cyber security implementation in organisation, it has to be risk-based approach (Von Solms, Basie & Von Solms, Rossouw, 2004). Risk management framework has been incorporated as an instrument to strengthen cyber security resiliency in the United States (The White House, 2013). For information security irrespective where the information is hosted in either on paper, electronic, or in cyber world, ISO/IEC 27001: Information security Management System (ISMS) has been used as a framework for information security (Veiga & Eloff, 2007). CNII sectors in In Malaysia through its Cabinet Directive in 2009, has directed identified CNII agencies to be certified under ISO/IEC 27001: Information security Management System (ISMS). ISMS implementation is deployed through risk based approach where information security risks can be minimized for both; information through cyber or non-cyber (e.g. on paper). In many organisations, ICT assets are owned by the ICT department or similar. However, these ICT assets are being utilised by users known as custodians who are responsible on the assets. This arrangement demands co-operation between users and custodians to ensure that assets and information in the assets are protected.

ISMS has demonstrated its capabilities in reducing risks and threats of information (Dey, 2007). In fact, ISMS has gained the trust being the de facto standard of many organisations in managing information security. Besides providing a framework to govern information security, it is capable of embedding information security culture in organisations (Veiga & Eloff, 2007). According to a study conducted by Rocha Flores et al. (2014), the results indicate that efforts in managing information security can be coordinated through processes including risk assessment, controls implementation and effective monitoring of selected controls, which can be done through ISMS implementation.

Although organisations have shifted to cloud security for cost efficiency, organisations cannot wash off their hands. Global Encryption Trends reported that several critical findings related to cloud data are that data at rest on the cloud is not protected and organisations also do not even know where their data resides (Business Cloud News, 2016). These are critical findings as organisations cannot totally rely on the cloud provider; which can attract the attention of cyber criminals. Apart from significant terms defined in the arrangement between the organisation and cloud provider, cooperation between organisations and cloud provider should be fostered in developing the proper process which should be translated into a documented procedure. This process should be defined by security team and incorporated in the business function to be tested as part of the organisational business continuity plan. In fact, prior to formal arrangement between organisation and cloud provider, risk assessment should be conducted and terms of the agreement and controls should be defined in accordance to the results of the risk assessment exercise. This is to ensure that both parties are aware on each responsibilities and how to respond in the event of incidents occur. The increase of cyber security chain increases the risks for the information security to be breached or compromised. Due to the increased of governance regulations in cyber security, assessing risks and implementing security controls are deemed necessary (Saint-Germain, 2005; Suhazimah Dzazali & Ali Hussein Zolait, 2012; Veiga & Eloff, 2007). More importantly, risks related to classified data hosted in the cloud platform should be prudently managed where data to be sanitised once the contract expires.

5.5.3.2 Security Vulnerability Management

The results of this study are also supported by Mohammed et al. (2015) where requirements set by Federal Information Security Management Act (FISMA) in the United States of America indicate the needs for security assessment to be conducted periodically in organisations to identify areas for improvement. FISMA, a piece of legislation in the US defines a comprehensive framework to protect government's information, operations and assets against natural or man-made threats. Security vulnerability management is a proactive security process that evaluates security aspects of ICT measures that have been implemented including technology, people and processes.

It is common in security environment that cyber security breaches can occur when vulnerabilities either humans or non-humans are exploited. Evidence from previous studies suggested that detection activities could assist in identifying potential computer abuse that cause vulnerabilities to exist (Straub Jr & Nance, 1990). One of best security practices in managing vulnerabilities is by assessing its security posture that includes assessing vulnerabilities at all security levels; network, application, servers and databases. The network, web sites and web applications will also be tested through penetration testing. Compliance to regulatory requirements does not guarantee that an organisation is secure. Despite complied with regulatory requirements, several incidents experienced by Target suggested that there is a need to conduct penetration testing in addition to the existing security compliance programmes in the organisation (Basu, 2014). Apart from having vulnerabilities were assessed to avoid being exploited by attackers, users in organisations are also required to cooperate in ensuring their systems are protected such as through patching the updates and downloading signatures for the anti-virus regularly.

Due to the non-exclusivity of vulnerabilities information, these information can pose security threats to others. Although this information is made available for system users to patch their systems in order to protect them (Radianti, Rich, & Gonzalez, 2009), this information can be easily abused as well. There are parties who misuse these information by creating exploits and sell these exploits in black market and to parties who needs these exploits in order to attack others (Lemos, 2015; Radianti, Rich, & Gonzalez, 2009).

5.5.3.3 Business Continuity Management

Another significant process that demands cooperation among employees in organisations is Business Continuity Management (BCM). Its significance has made BCM as part of board agenda in many organisations. Having BCM in place will not only minimize impacts of service disruption, but also allow organisations to continuously provide their services to ensure they stay resilient. In the context of information security, information as critical assets in organisations needs to be suitably protected online or offline to ensure its availability for business processes. BCM has been identified as one of security controls in the domain of ISMS in assuring the availability of information for organisations to operate while they are in disasters. Several service disruptions under the CNII umbrella require close attention where there have been such incidences such as suspension of trading by Bursa Malaysia (Bursa Malaysia, 2008) and services disruption by the light railway transit due to a technical glitch in their systems that affected the public (Ida Madieha Abdul Ghani, Sonny Zulhuda, & Sigit Puspito Wigati Jarot, 2012). Although the impact of the latter is rather physical, it provides an example of how the failure of ICT system do not only have direct effects on the systems operation, but indirectly affect the public.

According to Holowachuk (2007), cooperation is fundamental among business units in its implementation involving critical tasks. In the context of BCM implementation, it includes identification of organisational critical business functions and consistent rehearsals of these business functions. The former requires identification of resources, information and interdependencies for business functions to continuously serve stakeholders in the event of services disruptions while the latter emphasizes exercising recovery and continuity plans of these business functions. Cooperation is not only required internally, but also with vendors particularly towards the final developments of continuity plans (Rozek & Groth, 2008).

Results of this study are supported by Aronis and Stratopoulos (2016) where cooperation is crucial for IT department to work with other departments in rehearsing recovery procedures through simulation in the event of cyberattacks. It is critical to ensure that business function owners are familiar on what to be done as required in their continuity plans and procedures when disasters strike. One critical aspect of business continuity that demands participation and cooperation from all employees is exercising or rehearsing recovery and continuity plans. It is critical to ensure that business function owners are familiar on what to be done as documented in their continuity procedures when a disaster strikes. Critical business functions that are required to be exercised include among others ICT functions, core services, crisis communication IT disaster recovery and data recovery. These exercises are performed in routine that requires cooperation at all levels in an organisation. Not only exercising provides familiarity of what to be done in the event of a crisis, but also enhance employees skillset as exercising provides opportunities for improvements. Frequently, during a disaster, even employees who are not affected are required to extend their full cooperation by not disclosing information and speaking to external parties to avoid wrong perception that could create unnecessary rumours in worsening the situation. Thus, exercising is crucial for employees to exercise their roles and responsibilities in the events of crisis based on what they have learnt through the exercises conducted. This is supported by Nelson and Winter (2002), where learning from routine and skills and practicing those for perfection are capable of addressing behavioural continuity.

BCM has evolved from physical focus of disaster to disaster contributed by cyber security breaches. Components in BCM implementation demands a structured process for organisations to follow either in peace or crisis time. One of its critical components is data backup and recovery strategy that should be in place. A number of incidents related to loss of data is predictable, but is avoidable when critical business functions are tested and rehearsed periodically or as and when needed. For example, an incident happened while a migration process took place in University Malaya Medical Centre where approximately 46,000 electronic images of X-rays and scans of patients were wiped off (The Sun Daily, 2014). This can be avoided if process of migration and its sub-processes are documented and tested accordingly. In responding to the recent threat of “ransomware”, it can be addressed by performing a consistent back-up to ensure its availability at all times.

BCM components demand human cooperation that foster its deployment to meet the sustainability of organisations. In BCM, cooperation with external parties in also regarded as a continuity strategy that is known as reciprocal arrangement. This arrangement is usually deployed between organisations that share rare or unique business functions such as security laboratories in evaluating security products

5.5.3.4 Incident Management Procedure

In order to minimize the impact of security breaches, it is imperative for the incident to be responded as quickly as possible to recover the situation, eventually minimize the impacts the breach may have on the systems. An established cyber security management procedure includes an approved Incident Management Procedure (IMP) to handle incident and an established Computer Emergency Response Team (CERT) team that will be responding to security breaches. The IMP provides a platform for organisations not only to provide critical response to security breaches, but also provide steps to contain and recover the system back to normal. Two security incidents management standard; ISO/IEC 27035 and NIST 800-61 offer organisations the ability to plan and prepare for security incidents and responds through structured steps identified in the documents. Although they are not exactly the same, most common activities in handling security incidents are similar; plan, prepare, respond, contain, eradicate and lessons learnt (International Organization for Standardization, 2011; National Institute of Standards and Technology, 2012). The needs for organisations in critical sectors to establish cyber security incident management process has been described in various national cyber security related policies (Line, 2013; National Security Council, 2012; The White House, 2013). CNII organisations through one of the guiding principles defined in National

Security Council (NSC) Directive No. 24, is required to establish Computer Emergency Response Team (CERT). CERT together with established IMP creates the importance of managing cyber security incidents at organisational level before the incidents become accumulated at sectoral level that could lead to cyber crisis to the country (National Security Council, 2012). Although almost all respondents claimed that they were aware of the significance to have a CERT team, several have not yet the team established due to challenges in budget and skilled resources.

The findings of this study are also supported by Ahmad, Hadgkiss, and Ruighaver (2012) where senior management, security team, and IRT at certain points would cooperate in negotiating priorities and actions be taken while in the process of responding to security breaches. These findings were also concurred by (Johnson, 2014; Line et al., 2008), where they asserted that to recover from security incident, cooperation is required not only within the organisation, but also with external counterparts. Delay in responding to security breaches can give devastating impacts on organisations. In responding to incidents, the CERT cooperation between different sectors and association with other CERT teams and security vendors are also important. This form of co-operation is not only critical during the crisis time when incident has occurred, but also in peace time as this cooperation allows exchange of cyber security related information; threats, vulnerabilities and risks. Referring to incident of safety-critical software in the aviation industry, cooperation between safety management and teams of engineering and operational is needed as much as with external service providers (Johnson, 2014).

Cyber security breaches can be detected by employees who should report them as outlined in the IMP. By reporting them immediately, the security team can quickly respond and contain the breaches from spreading. It also reflects cooperation among employees. When employees reported security breaches, this should not be regarded as a negative perception where controls are being breached such as fault findings. Instead, it should be viewed as positive effects where; firstly the awareness programmes have been effective where employees know what have been breached and know how to respond to it and secondly, employees have been cooperative in reporting the breaches. Thus, reporting incident should be regarded as one of the metrics in measuring the effectiveness of awareness programmes.

Having users to cooperate in reporting cyber security incidents efficiently, awareness is not sufficient. It requires a structured incident management procedure to be in place and be rehearsed in a proactive manner. So, the employees can react smoothly in accordance with the procedure. Having clear roles and responsibilities defined in job functions for employees assigned to handle security incidents is also important for them to be prepared minimizing impacts in organisations. Thus, an established incident management procedure with established incident response team (Ahmad, Maynard, & Shanks, 2015) or Computer Emergency Response Team (CERT) to respond to security breaches is fundamental to provide a platform for various business units in managing security breaches effectively. The procedure is not only critical to respond to cyber security breaches, but to also provide lessons to be learnt to avoid future breaches (He, Johnson, & Lu, 2015; Shedden, Ahmad, & Ruighaver, 2010). Lessons learnt from the incident are important to avoid similar issues from happening in the future and should not be limited to only high impact incidents (Ahmad, Hadgkiss, & Ruighaver, 2012). The learning process to deter potential security breaches should be employed right from as low as little non-compliant to when the security breaches occur. Learning from experiencing security failure is an effective approach to continuous improvement in the whole process of information security management (Juhee & Johnson, 2014). Another process that is critically related to incident management is digital evidence collection procedure. Organisations need to also be prepared so digital evidence can be appropriately identified, collected, acquired and preserved in understanding the root cause of the security incident (International Organization for Standardization, 2012). This is one of significant components that many organisations have overlooked at despite having an established information security incident management procedure in place. Since cyber security is borderless, it also significant for this whole process to be conducted in accordance to accepted international practices. ISO/IEC 27037 is an international standard that provide guidelines to ensure that collected digital evidence is accepted in any court of law.

5.5.3.5 Security Processes and Interdependent Tasks

Both proactive and reactive processes above clearly shown the element of tasks interdependence that needs employees to cooperate. As discussed earlier, Guzzo and Shea (1992) were in view that for task interdependence to present there should be some degree of interactions and coordination among group members in completing their tasks where a mutual dependence is formed when the degree of interdependence is high (Ramamoorthy & Flood, 2004). Both proactive and reactive processes discussed above provide a significant degree of interactions and coordination among employees in performing their tasks while adhering to security policies and other requirements. The significance of having mutual dependence is that the goals of individualists and group can be closely aligned (Ramamoorthy & Flood, 2004) as they are implementing tasks in meeting a common goal.

In performing tasks, collectivism versus individualism introduced by (Hofstede, 1980, 1983) was applied in literature related to cooperation (Ramamoorthy & Flood, 2004; Wagner, 1995); where the former prefers to work in groups whilst the latter prefers to work individually. Collectivism reflects strong ties in groups where there is a presence of cooperation in the group (Ramamoorthy & Flood, 2004; Wagner, 1995) and individualists are those who are loosely integrated in the group where they are more concern of fulfilling their own obligations. In the cyber security ecosystem, individualists can also be associated with insider threats which is considered as one of the top cyber threats. Since individualists can be driven by personal motivations and interests, they tend to abuse the opportunities given to them. Distinct criteria of insider threats are that most of them have security roles and granted the trust in performing their tasks; who can be internal employees or external parties that are contracted out to perform such services. These criteria provide them ample opportunity to manipulate computer systems regardless their motives. According to PricewaterhouseCoopers (2016), almost half of the serious incidents that are related to economic crimes are due to employees who are hired by the organisations where these crimes are mainly motivated due to opportunity they were having in the organisations.

In the context on security processes discussed above, the cooperation required in those processes able to provide an environment that encourage consistent interactions and collective actions among employees in organisation thus deter those who are opportunists.

Not only new processes should be formally established in coordinating security activities as suggested by Rocha Flores, Antonsen, and Ekstedt (2014), these processes should also be announced, where the know-how of these processes can be communicated through training and awareness programmes. Kolkowska and Dhillon (2013), argued that failure in providing understanding of new security processes and requirements to users could lead to failure in changing their behavioural intention to follow the requirements.

Frequently, there is a need to have a balanced technology and human aspect investment to ensure information is highly protected in organisations. Since technology deployment requires human intervention through skills and expertise in manning them. Thus, these security experts need to cooperate not only with other technologies owners in other departments or branches (if the systems are decentralised), but also with technology providers. In situations where organisations have outsourcing arrangement with external parties, cooperation between outsourcer and outsourcing provider is paramount for this business arrangement to succeed (Mulej, Rebernik, & Bradac, 2006). Since outsourcing arrangement is built on trust, equal information sharing by both parties is significant for mutual benefits of both parties. In a situation where information asymmetry exists, one party may lead to opportunistic behaviour that would eventually leads to the failure of the business arrangement.

Cooperation is also extended to users who will be using these systems through training, awareness, educational programmes by providing necessary knowledge, information and rules to use the systems in a secure manner. Lack of formal components such as trainings and manuals for technical implementations may cause reluctance of employees to implement and perform such technical deployment (Musa, 2012). According to Ifinedo (2012), users are more likely to comply with security policies when they have relevant competence in implementing relevant preventive security measures. Deploying security technologies also demands cooperation from users to ensure it meets security objectives. A report by Verizon (2013) suggested that end users are still the most effective means in detecting security breaches.

5.5.3.6 Roles of Institutions

It is worth to note the roles of institutions in deploying good organisational practices in critical sectors to improve cyber security aspects in Malaysia; a cabinet directive that was issued by the Malaysian Cabinet on the 24th February 2010 on ISMS implementation and NSC Directive No 24 issued by the National Security Council in 2012 in providing guiding principles for cyber security in CNII sectors. The former required CNII organisations to manage security through ISMS implementation and later be certified to ensure cyber threats and risks are managed prudently while the latter provides guiding principles on cyber security measures for organisations to adhere to. Among these principles include ISMS implementation, CERT establishment and related capabilities and periodic security vulnerabilities assessment. One of the success factors for ISMS implementation is management commitment that needs to be demonstrated in complying with one of requirements in order to obtain certification. Through management commitment, provision to invest in security technologies and employees can be deployed for relevant security processes to be structured and established for users to adhere to.

Establishment of CERT in CNII organisations is a part of the National Cyber Crisis Management framework that requires cooperation from other entities in managing security incident before it becomes a crisis to the country (National Security Council, 2012). The significance of institutional role is also supported by Mohammed, Mariani, and Mohammed (2015) where requirements set by FISMA shows the significance for security assessment to be conducted periodically in organisations for security improvement. Apart from having vulnerabilities that were to be assessed to avoid exploitation by attackers, users in organisations are also required to cooperate in ensuring their systems are protected by patching security updates and downloading signatures for the anti-virus regularly; which are frequently stated in organisational information security policy.

5.6 Summary

Using the mediation results from research question two, North's (1991,1994) definition on institutions and learning respectively and ISMS (International Organization for Standardization, 2013) as the foundation, we examined the influence of the mediating variable (cooperation) on organisational security practices to cyber security compliance. Out of three organisational practices tested, all explanatory variables except SI were significant. Both TMC and SSP have both direct and indirect effects on security compliance through the intervention of cooperation.

Tasks interdependencies in security processes demand co-operation in organisations through deployment of both proactive and reactive approaches, in which neither of these approaches should be implemented in silos. In this study, we identified five distinct processes leveraging ISMS as the foundation in forming up an integrated security processes that require cooperation. Although ISMS is mainly observed as process centric, it provides a holistic security practices that requires both proactive and reactive approaches which are derived in the form of security controls as the outcome of the risk assessment exercise. Learning experiences from both approaches; learning from rehearsing and security failures both provide improvement in organisations to stay resilient in the fast changing threats of cyber security ecosystem. For security processes to be effectively deployed, relevant skills and competency should be developed and accordingly enhanced to ensure they are relevant. According to Nelson and Winter (2002), behavioural continuity of employees can be achieved through learning from routine and skills and practicing those for perfection. Thus, security processes such as business continuity management and incident management provide the demands continuous rehearsal and exercise not only contribute, but also assist resistance to change.

Although SI is not mediated through cooperation, it is positively associated with compliance. SI on technology and people requires cooperative efforts by both domains to remain useful in benefiting the money spent on organisations. However, this was not significantly found in this study.

The non-excludable characteristic of cyber security and cooperation through collective efforts by employees provides a synergy that attributed to the adherence of security requirements in organisations. The problem of cyber security that stems from the non-excludability aspect of public goods can be overcome by encouraging employees to cooperate; thus provides an avenue to assess behavioural compliance from a different approach. The findings also show the importance of institutional role in shaping organisational behaviour towards compliance. Using the definition of institutions and learning by (North, 1991, 1994) and organisational behavioural change (DiMaggio & Powell, 1983), this study demonstrates the importance of institutions in transforming CNII organisations to risk averse organisations. The role of institutions has also been found to be effective where there has been an increase in number of organisations obtained ISMS certification in Malaysia from 62 in 2010 (*ISO/IEC27001*, n.d.) to 262 in 2017 (Department of Standards Malaysia, 2017). The increase also demonstrates the pressures of mimetic isomorphism where other organisations follow the adoption of ISMS in CNII sectors in becoming risk averse organisations.

The results of this study show that it is able to fill the gaps left by previous security studies where cooperation is the critical component that influences organisational practices in contributing to security compliance in organisations. Although there were no previous information security studies emphasized cooperation as the mediating factor between organisational security practices and cyber security compliance, this study shows that the latter could be better achieved when employees do not work in isolation or detached from the rest of employees in an organisation.

CHAPTER 6: GOVERNING CYBER SECURITY AT MULTIPLE LEVELS

6.1 Introduction

The increase of cyber security incidents worldwide in early 2000 has triggered an institutional change in the governance structure of cyber security particularly in the Critical National Information Infrastructure (CNII) sectors in Malaysia. As deliberated in sub-section 1.7, there are ten (10) such sectors in Malaysia. In year 2006, Ministry of Science, Technology and Innovation (MOSTI) has devised the National Cyber Security Policy (NCSP) and it was handed over to the National Security Council in 2011 as it was responsible in national cyber security (Shamir b. Hashim, 2017). This policy has introduced the role of sector leads which has become increasingly important in the CNII sectors. The focus of this chapter is on the governance of cyber security at multiple levels in these areas. Multiple levels refers to three levels, namely, the national level, the sectoral level and the organisational level.

In addressing the research question 3, this study adopted quantitative and qualitative approaches as discussed in sub-sections 3.3.1 and 3.3.2. To analyse the quantitative data, this study used Ordinal Logistic Regression (OLR) as deliberated in sub-section 3.4.3. In complementing the quantitative findings[10], the following organisations were examined based on their role at each level. The central authority studied is Organisation VIII, the institution that provides directives and policies related to CNII sectors. There were three sector leads being investigated in this study namely, firstly, Organisation I in the government sector, secondly, Organisation II in the financial sector and thirdly, Organisation III in the healthcare sector. In addition, three other CNII organisations were

[10] The rationale for performing qualitative method in answering research question 3 is discussed in sub-section 3.3.

studied, first, Organisation IV in the information and communications sector, second, Organisation V also in the information and communication sector, and third, Organisation VI in the financial sector. The fourth organisation is Organisation VII which falls under the education sector and is regulated by Ministry of Education. However, Organisation VII has been guided by MAMPU on the ICT security aspect.

Therefore, the term “national level” refers to the central authority which is Organisation VIII. This is followed by the “sectoral level” and “organisational level” which comprises all the three sector leads and all the four organisations respectively as mentioned above.

Although CNII sectors in Malaysia have been a topic of interest by security scholars (Ida Madieha Abdul Ghani, Sonny Zulhuda, & Sigit Puspito Wigati Jarot, 2012; Zahri Yunos et al., 2010), little has been done to explain the efficacy of instruments used to achieve cyber security compliance in the three different levels of organisations governing cyber security: at organisational, sectoral and national levels in these sectors. Hence, the objective of this chapter is to examine the existing governance instruments implemented at these levels that contributed to cyber security compliance in organisations. In the NSC Directive No 24 (NCS 24), applicable throughout all ten (10) CNII sectors, including the three mentioned above, decentralisation has been recommended as a governance tool in managing cyber security. The decentralisation process in governing the sectors through the sector leads has helped NSC in implementing the eight (8) policy thrusts as defined in the national policy. Since then, being the central authority, NSC has enhanced the scope of cyber security to cover all aspects of security on the Internet that could threaten the national security. In the context of this study, national security interests cover cyber security attacks and incidents related to these critical sectors that may have an impact on five areas, namely, national economic strength, national image, national defence and security, government capabilities to function and public health and safety. [11]

Although the role of sector leads and the central authority were clearly defined through the National Security Council Directive No. 24 (NSC24), there are some confusions over the governing activities of the three sectors mentioned above. There was an absence of a clear direction on monitoring and reporting of cyber security efforts by NSC on the three sector leads. This has created a vacuum that requires attention in strengthening these sectors. Hence, the sector leads took their own initiatives and did their own cyber security monitoring through their own channels for CNII organisations under their purview.

This chapter is made up of six sections. The next section presents the theoretical considerations essential to examine governance instruments in CNII sectors in Malaysia. Section three discusses variable measurements. This is followed by section four on the findings and discussion and finally the summary of this chapter in section five.

6.2 Theoretical Considerations

An analytical framework that reflects the three levels is presented in Figure 6.1. This analytical framework addresses instruments that are associated with governing cyber security at these levels. At the highest level of the governance structure, instruments that were examined include statutory acts and national policies, circulations and directives related to cyber security in terms of their sufficiency and effectiveness. Similarly, at the sectoral level, sufficiency and effectiveness of directives and circulars pertaining to the sectors are examined. At the organisational level, this study examined three instruments;

[11] These five impacts area are deliberated in the NCSP and NSC24 in sub-section1.2.2

established information security governance structure, security leadership and information security audit.

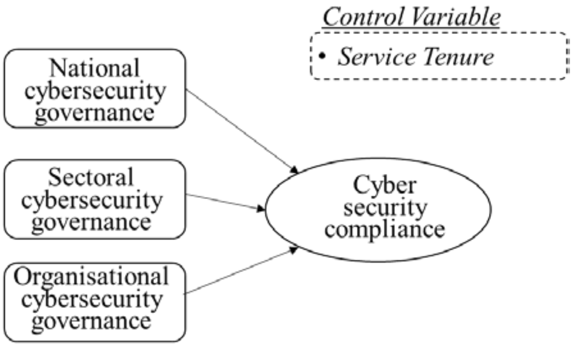

Control Variable
• Service Tenure
National cybersecurity governance
Sectoral cybersecurity governance
Organisational cybersecurity governance
Cyber security compliance

Figure 6.1: Analytical Framework of Cyber Security Governance in CNII Sectors
Source: Author

6.2.1 Existing Governance Instruments at the National Level

At the national level, there are two categories of instruments that govern cyber security activities in CNII sectors; statutory requirements and non-statutory requirements. The statutory requirements are related to cyber related acts which do not only apply to CNII sectors, but also to all Internet players in the country. However, for the purposes of this study, these requirements were also examined. The non-statutory requirements examined were two main policy documents issued by NSC namely, the NSC Directive No 24 (NSC24) and National Cyber Crisis Management Response, Communication and Coordination Procedure (NCCMRCCP). The former that was previously discussed in sub-section 1.2.2.2 provides guiding principles to ensure CNII sectors are well-protected in cyber space and the latter instrument provides guidance for CNII sectors in response to cyber security incidents. In addition, a Cabinet Directive to implement ISMS that later to obtain certification based on the ISO 27001 standard was also studied. The reason being was that these three instruments demand huge involvement, participation and cooperation of CNII organisations, sector leads and NSC.

6.2.1.1 National Cyber Crisis Management Response, Communication and Coordination Procedure

Due to its interconnectivities and the cascading effects an incident may have in these critical sectors, cyber security incidents need to be effectively managed at all levels to avoid it from becoming a crisis to the country. Thus, in ensuring its readiness at every level in these sectors, the NSC has developed the NCCMRCCP that demands cooperation amongst sector leads, CNII agencies, NSC and other relevant stakeholders in the event of cyber security breaches. This national procedure provides a standard operating procedure for CNII organisations to respond to cyber security incidents occurred in these sectors.

6.2.1.2 Cyber Security Statutes in Malaysia

There are statutes that are applicable in governing the Internet activities in Malaysia. There are two prominent acts related to information security; Computer Crimes Act ("CCA") 1997 and Communications and Multimedia Act (“CMA”) 1998. CCA is the first statute related to information security which is punitive in nature whilst CMA is more administrative that provides a single regulatory framework for convergence of three different industries; computing, telecommunications and broadcasting and computing (Sonny Zulhuda, 2012).

The most fundamental attribute of the Internet is its borderless nature. Thus, for any security breaches occurred, it is crucial to understand what causes the breaches and where the attacks come from. What matters most after security breaches is the preservation of evidence in ensuring it is admissible in any court of law. Due to this, in 2012, the Evidence Act 1950 [Act 56] was amended incorporating Malaysian Government’s concern on Internet activities where the term 'computer' has been amended as follows:

> *An electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing*

> *logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include (a) an automated typewriter or typesetter; (b) a portable hand held calculator; (c) a device similar to those referred to in para (a) and (b) which is non-programmable or which does not contain any data storage facility.*

For the same act, a new section 114A (also known as Evidence (Amendment) (No. 2) [Act 1432] was introduced by the Malaysian Government as it was necessary to protect the interest of the public. This is due to the increase of defamation issues on the Internet with the anonymity of the Internet users as the stumbling block. The Malaysian Government viewed this amendment as being able to assist in manning this issue thus, providing proof of the identity of Internet users. The amendment was also meant to assist in proving the offences against Internet users under the other relevant statutes; the Communications and Multimedia Act 1998, the Computer Crimes Act 1997 and the Sedition Act 1948. ("Evidence (Amendment) (No 2) Act 2012," 2012). Section 114A, of Evidence Act was passed by Dewan Rakyat and Dewan Negara in April 2012 and was gazetted on 31st July by de facto law Minister Mohamed Nazri Abdul Aziz (Centre for Independent Journalism; Mohamed, 2013).

According to Condon (2010), the new section 114A of the Evidence Act 1950 creates a presumption that any registered user is presumed to be the publisher of any publication in blogs, news or social media that is sent from their computer unless the user is proved otherwise. New Section 114 A of the Evidence Act provides for “presumption of fact in publication” which allows a Court of law to assume that any of the following persons is the author of a publication: firstly, a person whose name, photograph or pseudonym appears on any publication depicting himself as the owner, computer host; secondly, any person who is registered as a subscriber with the Internet Service Provider, and thirdly, any person who has in his custody or control any computer from which any publication originates ("Evidence (Amendment) (No 2) Act 2012," 2012). In other words, an Internet user is deemed to be the publisher of the content unless they can prove that they did not publish them. This is contradictory with the norm of legal proceedings where a person will not be found guilty unless he or she is proven otherwise. With this new amendment, the burden of proof has been shifted to the Internet users. Victims of hacking and identity theft must provide evidence that they were not the ones who caused the crimes. This has caused a public outcry amongst the Internet community in Malaysia. Without sufficient awareness on using the Internet, this amendment makes most Internet users (who are not prudent while being on the Internet) pay the price for actions they did not commit.

6.2.2 Existing Governance Instruments at the Sectoral Level

In dealing with cyber security, roles of institutions are significant to curb illicit security activities; thus significantly complementing security efforts done by organisations. In CNII sectors in Malaysia, the role of sector leads is important in regulating their respective sector to ensure regulatory instruments such as policies, directives and circulation were available and sufficient for organisations to follow and adhere to.

Although sectors have their own policies related to their core operations, for purposes of cyber security, these sectors mainly relied on the centralised cyber security related policies and directives such as the NCSP, NSC24, NCCMRCCP and CDISMS[12]. Sector leads were responsible for identifying organisations under their purview as CNII organisations, based on criteria which they have set. A list of these identified

[12] These policies directives (NCSP, NSC24 and CDISMS) were discussed in sub-section 1.2.2

organisations were later furnished to the central authority for consolidation in 2012 with the purpose to keep them as a database for the Organisation VIII's related programme. The list were updated from time to time.

Being a government entity that is responsible for ICT and information security for the government sector, Organisation I has established a Government Security Operation Centre (GSOC) and a Government Computer Emergency Response Team (GCERT) that provide centralised security services to government agencies particularly to those agencies which Organisation I provides budget allocation for their ICT resources. The former provides security threat monitoring services where alerts would be issued for anomalies detected in their systems that could harm the government network. These alerts would directly notify those affected organisations through emails for immediate action, and the copy of this notification would also be emailed to respective sector leads. GCERT is a centralised team for managing cyber security incidents in the government sector. When an incident occurs, it would be directly reported to GCERT where incidents would be responded to. In both situations, Organisation I would be doing the monitoring instead of respective sector leads. Whenever security alerts sent to affected agencies by the GSOC team, their respective sector leads would be notified. However, this was not aligned with what has been outlined in NSC24 and NCCMRCCP where sector leads were required to do security monitoring for agencies under their purview in both peace and crisis times.

There were circumstances where sector leads were required to do close monitoring of security events for their sector in accordance to the NCCMRCCP. However, this was very rare and only happening when there were potential threats to the nation's security such as anonymous attack in 2012.

6.2.3 Existing Security Governance Instruments at the Organisational Level

At the organisational level, three security governance instruments were examined; firstly, security leadership, secondly, established security governance structure and thirdly, information security audit. The prevalence of these three governance instruments stem from the relevant national policy documents namely, NSC24 and ISMS Cabinet Directive. NSC24 discusses two critical positions that reflect security leadership in attending to ICT security related matters in CNII organisations namely; Chief Information Officer (CIO) and Certified Information Security Officer (CISO). Both positions are responsible of security related matters in their organisations. However, CIO has added responsibilities to provide leadership in steering ICT strategies and implementation. In the government sector, all agencies are led by CIOs in determining ICT strategies for their organisations and ensure its implementation.

Established information security governance structure is evident through the implementation of ISMS. One of security requirements in governing information security related matters in organisations is to establish security governance structure together with defined roles and responsibilities in ensuring security requirements are adhered to (International Organization for Standardization, 2013).

The direction of the Malaysian Government for CNII organisations to achieve information security certification requires organisations to go through information security audit exercise (Zahri Yunos et al., 2014). Not only this exercise can check compliance against security requirements based on ISO/IEC 27001 (Razana & Shafiuddin, 2016), but can also become a tool to check cooperation amongst employees in working towards obtaining certification for the organisation. The importance of conducting information security audit is evident as it provides profound security improvement in organisations.

6.3 Variable Measurements

To operationalise the constructs in answering the third research question, we adapted some items from previous relevant studies as discussed below. We also developed new constructs that were not published before. We measure cyber security compliance (CSC), which is the dependent variable by assessing the likelihood of the respondents' organisations of achieving cyber security compliance with the present level cooperation available in organisations. In the survey, information about CSC was obtained and coded in a 5-point Likert scale namely: 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree and 5= strongly agree. In providing clarity of responses of the dependent variable (CSC), relevant scale items were collapsed into 3 categories; where (i) responses on strongly disagree and disagree were combined and coded as 1 = disagree, (ii) neutral responses remained as 2 = neutral and (iii) agree and strongly agree responses were combined and coded as 3 = agree. There are three explanatory variables and one control variable used to answer the third research question. See Appendix A section 2.

Independent variables were selected in accordance with governance instruments deployed at three different levels; organizational, sectoral and national levels. At the organizational level, the independent variable is a construct comprised of three instruments based on three items; established security governance structure (ESG) (International Organization for Standardization, 2013; Kayworth & Whitten, 2010), cyber security leadership (CSL) (ISACA, 2011; Kayworth & Whitten, 2010) and information security audit (ISA) (Kayworth & Whitten, 2010; Steinbart et al., 2012; Vroom & Von Solms, 2004). These items for the organisational level were measured as single items and coded in a 5-point Likert scale namely: 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree and 5 = strongly agree. These items were later transformed into a construct as the independent variable for organisational level, Organisational Cyber Security Governance (OCSG).

There were hardly previous works related to this study in validating measurements of security governance instruments at both sectoral and national levels. Thus, independent variables were developed by specifically tailored to the context of these CNII sectors. Independent variables for sectoral and national levels were in the form of constructs; National Cyber Security Governance (NCSG) and Sectoral Cyber Security Governance (SCSG). These constructs were measured as continuous variables and established by summing and averaging the respective scale items. The construct of the SCSG was established based on two items; sufficiency (SLC1) and effectiveness (SLC2) of governance instruments deployed at the sectoral level. The items did not specify the exact instruments defined by the sectors. Instead the items were described in a general manner to reflect the roles and responsibilities of relevant institutions in governing CNII organisations under their purview.

At the national level, the NCSG was established based on five items revolving around existing cyber security regulations (CSR1 and CSR2) and the role played by the presence of the central authorities (CSR1, CSR2 and CSR3) pertaining to cyber security in CNII sectors in Malaysia.

6.4 Results

In answering the third research question, the findings are categorised into two categories; descriptive and statistical analysis. Descriptive analysis are based on demographic variables whereby the statistical analysis are findings based on the OLR conducted which are discussed in the next sub-sections. Findings from the interview are deliberated in the discussion section to complement the statistical results.

6.4.1 Descriptive Analysis

In terms of quantitative analysis, sample demographic characteristics are deliberated in sub-section 4.4.2. As for data normality, the Jarque-Bera test was performed prior to determination of the analytical method in performing the analysis. Data normality analysis was discussed in sub-section 4.4.4. Because the data was not normally distributed, it did not meet the assumption for linear regression testing. Hence, we used ordinal logistic regression to analyze the data. Missing data was later assessed where less than 10 percent missing data was detected in random fashion which was acceptable (Hair et al., 2010).

In testing the internal consistency of the variables, the Cronbach value was computed where the results show that the computed values are 0.7 and above. The Cronbach coefficient alpha values for measuring OCSG (0.707), SCSG (0.706) and NCSG (0.781) indicated acceptable reliability values (Moss et al., 1998; Nunnally, 1978).

The descriptive statistics of the variables used in this study were exhibited in Table 6.1, where statistics specific to OCSG, SCSG and NCSG were presented. We summarised the findings as follows. Firstly, 70.9% respondents reported that they agree that CSC was achieved in their organisations, followed by those who were neither disagree nor agree (21.29%) and 7.74% who disagree that CSC was achieved. The average response of all explanatory variables with standard deviation did not have great variance where NCSG (mean= 3.75, SD= 0.78), SCSG (mean= 3.73, SD= 0.92) and OCSG (mean= 3.67, SD= 0.73) were found.

In the model diagnostic tests, the check of multi-collinearity indicated that multi-collinearity did not exist. The Variance Inflation Factor (VIF) of independent variables were less than 2 where the recommended value for multi-collinearity is less than 3. The parallel test lines produced the p-value that was more than 0.05 (p = 0.996) which indicated that there was no issue with the suitability of the model. The p-value of less than 0.05 indicates that the model was not suitable which could be due to wrong link function that could affect the ordering of the dependent variable's categories (Chan, 2005). Since the parameter estimates did not produce the Odds ratio (OR) value, the value of OR was computed by exponentiating the coefficient estimates (Chan, 2005). The same method was also performed to compute the Confidence interval (CI) for the Odds Ratio.

Table 6.1: Descriptive Statistics of the Variables Used for Ordinal Logistic Regression

	n, (%)	**Mean, (SD)**	**Disagree (n, %)**	**Neutral (n, %)**	**Agree (n, %)**
Cyber security compliance [a]	155, (100)	2.63, (0.62)	12, (7.74)	33, (21.29)	110, (70.96)
Cyber security governance at national level (NCSG)[b]	155, (100)	3.75, (0.78)	-	-	-
Cyber security governance at sectoral level (SCSG)[b]	155, (100)	3.73, (0.92)	-	-	-
Cyber security governance at organisational level (OCSG)[b]	155, (100)	3.67, (0.73)	-	-	-
Service Tenure					
Less than 2 years	22, (14.19)		1, (0.65)	3, (1.94)	18, (11.61)
Between 2-5 years	28, (18.06)		2, (1.29)	5, (3.23)	21, (13.55)
Between 6-10 years	45, (29.03)		3, (1.94)	9, (5.81)	33, (21.29)
More than 10 years	60, (38.70)		6, (3.87)	16, (10.32)	38, (24.51)

Note:
n- total observations, SD=Standard Deviation
[a] The dependent variable was measured by Likert scale which was later collapsed into 3 categories: Disagree, Neutral and Agree
[b] These independent variables were measured by the Likert scale (from 1=strongly disagree to 5=strongly agree)
Source: Computed from the Author’s Survey

6.4.2 Results of Ordinal Logistic Regression

The results show that cyber security governance instruments implemented at both organisational (OR = 2.469, p = 0.000) and national (OR = 4.242, p = 0.005) levels were found to be effective and significantly contributed to CSC in CNII organisations. However, instruments implemented at sectoral level were found not to be significant (See Table 6.2).

Based on the OLR analysis conducted, the results show that the co-efficient for NCSG was 1.445 which is statistically significant at 1% significance level and positive, indicating that for every unit increase in NCSG, there is a 1.445 increase in the log odds of being in a higher level of agreeableness (i.e., moving from "disagree to neutral" or "neutral to agree") that cyber security governance instruments have been effective towards achieving CSC in organisations given all of the other variables in the model are held constant. The cumulative odds ratio is exp(1.445)=4.242, which means that when passing from disagree to agree that CSC is achieved, there is an increase of 4.242 times that national governance instruments were effective in achieving compliance. This indicates that the instruments provided by the central authorities encompassing relevant circulars, policies and directives were effective in regulating CNII organisations at the national level.

Table 6.2: Ordinal Logistic Regression Results for Effectiveness of Governance Instruments Implemented at Organisational, Sectoral and National Levels

Variables	**Coefficient, β**	**Standard Error (SE)**	**Odds Ratio (OR)**	**(95% Confidence Interval) for Odds Ratio**
Cyber security governance at national level (NCSG)	1.445***	.283	4.242	(2.437, 0.7382)
Cyber security governance at sectoral level (SCSG)	-.272	.259	1.312	(2.179, 1.264)
Cyber security governance at organisational level (OCSG)	0.904***	.321	2.469	(1.315, 4.632)
Service Tenure				
Less than 2 years	1.111	.649	3.037	(1.173, 10.360)
Between 2-5 years	0.964	.580	2.622	(1.190, 8.174)
Between 6-10 years	0.935	.485	2.547	(1.016, 6.586)
More than 10 years	0^a		1	

Note: *** - Significant at 1% significance level
Source: Computed from the author's Survey

As for the cyber security governance at the organizational level, the co-efficient was 0.904 which is significant at 1% significance level and positive, explaining the cumulative odds ratio of the effectiveness of governance instruments implemented at OCSG level in achieving CSC are 2.469 times higher as CSC moves to the next higher category of the level of agreeableness (i.e., moving from "disagree to neutral" or "neutral to agree"), given all of the other variables in the model are held constant.

However, security governance instruments at the sector level were found not to be significant in governing CNII organisations in their sector. This could be explained where only a few sector leads that actually did provide relevant circulations and directives to their agencies in addition of the governance instruments provided at the national level. Based on this study, among the three sector leads studied, only Organisation I issued their own circulations and directives related to cyber security for their sector. Other sector leads are heavily reliant on directives issued by the NSC and also by MAMPU. To provide more clarity in understanding the sufficiency and efficacy of the governance instruments at the sectoral and national levels, interviews were conducted and deliberated in next sub-sections of this chapter.

The following sections discuss the governance of cyber security compliance; its achievement, issues and challenges at the three levels. All respondents that have been interviewed referred to ISMS as the framework for them to govern information and cyber security in their organisations. They have also made reference to the other two main documents; NCCMRCCP and ISMS Directive as explained above.

6.4.3 Governing Cyber Security in Organisations

This section deliberates the findings of this study that are associated with people centric that contribute for a better CSC in CNII organisations; an established cyber security governance structure, cyber security leadership, and information security audit.

6.4.3.1 Established Cyber Security Governance Structure

The establishment of cyber security governance security structure is important to ensure that CSC is achieved. Although information security is everyone's responsibility in any organisation, an established governance structure with defined roles and responsibilities should be in place. The results of this study are supported by Von Solms, Basie and Von Solms, Rossouw (2004) where the structure should define the personnel who are responsible for information security in the organisation together with their roles and responsibilities. It is normally hierarchical in a form that includes top management, middle management, technical management and employees. The author submits that this structure should also accommodate a committee that can be referred to information security management committee as part of the structure. The structure should also provide security roles and functions in managing information security in organisations.

The structure should provide a clear and defined reporting line of cyber security activities in organisations for cyber security efforts held in organisations. The structure should also provides directives in ensuring that security programmes meet the objectives of establishment of information security that aligns with the organisational objectives. Failure to meet security objectives indicate failure of the organisation to meet its organisational objectives since security objectives should be aligned with organisational objectives (International Organization for Standardization, 2013). According to Meyer and Rowan (1977), a structure established in an organisation for purposes of compliance with institutional requirements could influence the survival of an organisation.

Accountability and responsibilities of information security should be shared by all employees in the organisation (Von Solms, Basie & Von Solms, Rossouw, 2004). One of the means to ensure employees are aware is by defining information security responsibilities in their job description. By stating this, employees are automatically responsible for information security while carrying out their tasks. In fact, employees' responsibilities should be made clear even before they join the organisation, in this context, this information should be made known to them during the interview session.

Respondent6 stated that information security governance structure established in her organisation is hierarchical in nature comprising a board of directors, a management committee and an information security committee which is:

> *Cyber security in our organisation is being driven by top down approach. We have various committees that govern cyber security efforts and its implementation. Our information security related policies are endorsed by our board of directors. In terms of management system, the highest level is our management committee led by the group managing director. And from there we also have information security working committee or working group that consists of head of departments who actually do the implementation and also analytical and provide suggestions to the management on what to be improved further.*

The committee mentioned by Respondent6 is observed to ease the problem highlighted by Kritzinger and Von Solms (2005), where security problems can only be detected annually through information security audit exercise. Thus, having a platform to discuss security issues several times a year, it helps organisations to monitor the users' cooperative behaviour in complying with cyber security requirements.

Information security committee functions as a platform to discuss information and cyber security issues and progress in organisations that include effectiveness of security tools deployed, results of risk assessment exercise, non-compliance issues, audit and budget.

Respondent5 highlighted the role of the information or cyber security committee in improving security in her organisation as follows:

> *We have recently conducted an Information Security Management Committee (ISMC) meeting and discussed whether the existing tools were sufficient to detect cyber attacks. One of the members said that their team deployed "fiereye"- a system used to detect cyber threats as part of our collaborative projects. This "fireeye" could identify these threats and later blocked the attacks as our existing "website application firewall" was not capable of doing that. Actually, we have to improve in terms of security technologies deployment in our operation.*

An information security committee platform can also serve as a platform to ensure compliance monitoring and enforcement capability are in place. Frequently, results from a risk assessment exercise create opportunities to obtain budget allocation for cyber security implementation and improvement. Thus, budget requirements for implementing security controls can be tabled in this committee. Not only that, this committee is important to monitor the effectiveness of information security controls that have been implemented. Issues that have cropped up in the implementation especially when the controls involved owners from multiple departments, may be resolved in this platform. This committee can also be the platform to provide the necessary cooperation among information and risk owners, and provide information sharing on information security threats, vulnerabilities and incidents. Thus, this platform should be chaired by someone from the top management. It is of utmost importance that roles of top management are explicitly defined in the structure.

6.4.3.2 Cyber Security Leadership

The policy directive of NSC24 requires a CIO or CISO to lead cyber security initiatives in CNII organisations (National Security Council, 2012). In addition to this policy, a framework which defines information security professionals in CNII sectors in Malaysia identified a CISO as the highest ranking information security officer in CNII organisations (Ministry of Science Technology and Innovation, 2012). Having someone who is part of the senior management team is capable of influencing employees in adhering to security requirements is an important consideration in governing cyber security effectively.

Respondent2 explained that assuming the role of a CIO in the government sector is like assuming another role in addition to the existing role of the senior official who was appointed as the CIO in the government agency. She explained:

> *"The CIO is supposed to develop strategic plan and oversee everything about cyber security. But, one of the challenges in the government sector is that a CIO must be a post. The CIO post is like an extra responsibility, in addition to what they do at the senior management level. Not like in the private sector where in a company that has a CIO, it is a pure CIO. But, this is not the case in the government sector. MAMPU used to have programmes for CIO on what they are supposed to do etc. But now, it all depends on the individuals. If these individuals (CIO) want to look at ICT, they will. But, most of the times, it is left to ICTSO (ICT Security Officer). So the CIOs do not know much about what is happening".*

This suggests that CIOs in the government sector did not put high priority in cyber security aspect since they already have their primary role and assuming the role of CIO is considered as secondary.

However, there has been a mixed response relevant to the aspect of leading cyber security efforts in CNII organisations. According to Respondent5, apart from having CISO in her organisation, the involvement of their CEO in spearheading cyber security initiatives in their organisations helped to influence employees in achieving better security compliance. Organisation V is a related government agency under the purview of Ministry of Science, Technology and Innovation. Respondent5 deliberated how the CEO in her organisation took charge of security efforts as below:

> *In our organisation, our CEO plays an important role in overseeing the cyber security governance particularly its implementation. He is the chairman of the information security committee that provides a platform to discuss all issues of information security in our organisation. He is also responsible to provide directives and assignment of roles and responsibilities to staff. We also have a CISO, where amongst his tasks is to chair information security working group where we discuss information security efforts such as the establishment of Computer Security Incident Response Team (CSIRT), issues on internal audit, other technical issues and operational issue related to cyber security implementation.*

Previously, information technology or information security professionals were not represented in many of the top management groups in organisations (Andrew & Nada, 2000), but now these groups are part of the senior executive team, through the appointment of a CISO or CIO. Protection of information either in digital or non-digital format should be viewed as a business issue and not a technical issue (Von Solms, Basie & Von Solms, Rossouw, 2004). Thus, having someone at the top management level to lead security efforts such as an appointment of a CISO is crucial to drive security in the right directions that align with organisational objectives.

The importance of having top management in leading information security initiatives has been widely discussed in information security literature (Von Solms, Basie & Von Solms, Rossouw, 2004). The presence of a Chief Information Security Officer (CISO) or equivalent to lead cyber security initiatives organisations is crucial to prevent data breaches (Ponemon Institute, 2010). A CISO's role is very important not only to articulate cyber risks and decide the right approach in cyber security to top management, but also to convince them in presenting a business case for security investment.

The absence of a CISO can create adverse consequences to organisations. Security experts cite the Sony's case (Newman, 2011) as one of the lessons learnt, where in April 2011, a cyber security attack on PlayStation Network and Qriocity has caused services outage which provides evidence that relevant security practices, precautions and issues that were not addressed accordingly. Sony could have prevented this attack earlier with the presence of a CISO. Similarly, the absence of a CISO in Target Corporation has been identified as the root cause of the systems breaches in 2013 and 2014 (Boulton, 2014) that cost the organisation approximately US$1 billion (Seals, 2015). Thus, it is important to have someone who is from the top management level to lead and be responsible for the overall cyber security of the organisation. He or she should also have the relevant competence and skills to meet stakeholders' expectations.

These findings can also be viewed from the perspective of a cultural dimension. Although previous studies show that top management is a critical factor for better security compliance in organisations, the impact of leadership can be subjective to the power distance index that the organisation belonged to. In Malaysia, the power distance index is high (Merritt, 2000) which means that the tendency for subordinates to easily follow instructions is high. In the context of information security, by following blindly leaders who have little knowledge and capabilities in driving cyber security in organisation, the impact can be huge to organisations. Interestingly, Malcolm Gladwell (as cited in Ohlheiser, 2013, p. 3) concluded in his essay *Outliers,* that a hierarchical culture during pilot communication had caused more Korean Air planes crashed compared to other airlines during that time (Ohlheiser, 2013; Reingold, 2008). In the context of the Korean air incidents, the design of complex airplanes like Boeing and airbus required the fleet to be flown by pilots who were equal which worked fine in low power distance cultures (Ohlheiser, 2013). In other words, these fleets required pilots to communicate regardless of ranking where they could correct each other when necessary. However, this is not the case with pilots with Korean airlines. Due to high power distance in their culture, there were occasions where the co-pilot would not correct the mistakes made by the senior pilot; thus causing the incidents (Ohlheiser, 2013; Reingold, 2008).

Similarly, in the context of cyber security, the impacts of cyber security breaches can be huge, thus, top management apart from providing resources and support should also be well-equipped with relevant knowledge of security. In Malaysia, being the nation with the highest power distance index culture, it is possible that any critical decisions made will not be contested and corrected by subordinates including those responsible for security decision-making. This can cause threats to the organisations in Malaysia. Thus, inculcating a security culture is important for organisations at all levels, so employees have sufficient information and knowledge for being responsible and accountable.

6.4.3.3 Information Security Audit and Scoping

Information security audit has been known as a tool to demonstrate to regulators and enforcement agencies the efforts put by organisations in complying with security requirements. Thus, the findings of this study are supported by Kwon and Johnson (2011), where audit policies have significantly increased compliance levels for regulations such as HIPPA in the US.

Information security audit has also been frequently conducted to meet requirements to obtain relevant certification. For example, for organisations to be certified under ISO/IEC 27001, organisations need to conduct internal audit as well as to have a third party audit. Being certified does not necessarily guarantee that organisations are secured from cyber threats. One possible reason is not having the right scope for ISMS implementation and certification. Generally, ISMS certification process is based on the scope identified, which does not necessarily cover the whole organisation. Thus, to obtain ISMS certification, it is important for the right scope to be defined to ensure risks associated with the scope are managed and mitigated.

In associating a security breach that occurred in the government sector recently, Respondent1 reported:

> *There was a security breach reported in the ministry "A". One of the employees has intentionally disclosed confidential information to the public. But, their scope of the ISMS certification of the ministry covers only their IT department that did not take into account risks in other parts of their business environment. I think we need to revisit the scope.*

This clearly indicates that obtaining certification just for the sake of adhering to the directive without setting the right objectives can defeat its purpose. Thus, it is important to carry out a correct scoping exercise for ISMS implementation. Scoping or establishing ISMS scope means determining the boundaries and applicability of the ISMS within the organisation for its implementation. The scope for ISMS implementation should be carefully selected as the information security risk assessment exercise to be conducted will be based on the scope defined. Thus, in minimizing cyber security threats, the right scope of the ISMS implementation is important. Unfortunately, in responding and adhering to the Malaysian Cabinet Directive for ISMS implementation, many organisations defined IT department as the scope for the ISMS implementation. This gives a wrong signal in managing security where information security should be beyond the ICT aspect. Thus, wrong scoping can defeat the purpose of its implementation. Since ISMS is a risk-based approach, risks should not be limited to only ICT/IT department, but should cover the overall business environment where ICT supports business operations in many organisations.

For employees to comply with security requirements, security compliance checking and monitoring is essential. Due to emphasis on ISMS implementation in CNII organisations in Malaysia, information security audit has been acknowledged as a mechanism in checking cooperative behaviour of employees whether they comply with policies and procedures and other security requirements as set forth by organisations. Internal audit exercise is basically to check the adherence of employees not only in complying with the policies and procedures, but also with other security requirements as stated in the ISMS requirement clause of A.18 on information security reviews. Clause A.18.1 is to ensure compliance with legal and contractual requirements and clause A.18.2 is to ensure information security is implemented and operated in accordance with organisational policies and procedures (International Organization for Standardization, 2013). For organisations to be eligible for certification, an external audit will be conducted by an independent party. Although conduct of an information security audit will not guarantee that security breaches do not occur, it will help to mitigate the impact of non-compliance. The internal audit report should be presented to the top management of ISMC or similar for further actions. In addition to this understanding, in this study, information security audit is described as a tool to check cooperation and participation of employees in information security programmes held by organisations.

Early detection of security non-compliance can be resolved by a deep understanding of the root cause in correcting them. In an audit exercise, employees will be checked against their practices whether they adhere to security policies and procedures in doing their tasks (Kritzinger & Von Solms, 2005). When they followed and adhered to what had been outlined in security policies and procedures, this indicated that they cooperated with the owner of the documents. To ensure that information security audit exercise is effective, it needs to be planned accordingly. The involvement of top management and business functions owners is also mandatory. A report of audit findings should be made available to them for continual improvement.

Apart from a formal information security audit that is normally conducted once a year, some organisations conducted their own independent self-control assessment as stated by Respondent6:

> *We have also conducted self-assessment by providing a checklist on things that we need to comply. Different teams will check against each other using this checklist. This assessment is managed by our internal audit team and risk division which allow us to have this independent assessment exercise. After we did the self-assessment, an attestation was conducted on how effective the controls were implemented in our own department. The results were later submitted to our internal audit team and risk division for their review.*

One important aspect that has been discussed in prior studies related to audit is the emphasis on the internal auditor to possess relevant technical skills and knowledge

(D'Onza, Lamboglia, & Verona, 2015; Steinbart et al., 2012) and the integration of the skilled auditors with the business processes (D'Onza, Lamboglia, & Verona, 2015). This is to ensure that the auditors are able to ask the relevant questions while performing the audit exercise. However, this study argues that in auditing information security, it requires a multi-disciplinary skillsets related to information and cyber security because it is not only about technology, but it is also about process and people. Thus, ISMS implementation provides a mechanism to audit all these three aspects in mitigating cyber and information security risks.

ISMS audit findings would trigger further opportunities for continual security improvement. For example, if the findings point to the needs to have systems vulnerabilities assessed, then a vulnerabilities assessment should be conducted. Steinbart et al. (2012), postulate that in conducting information security audit, the approach should be more towards consulting rather than policing by the internal auditors. In this way, the mutual trust between information security owners and the auditors can be increased; thus increasing the level of cooperation between them (Steinbart et al., 2012).

6.4.4 Governing Cyber Security at the Sectoral Level

The findings from the quantitative analysis of this study indicates that instruments produced by the sector leads are neither sufficient nor effective in contributing towards security compliance in CNII organisations. There are mixed responses in relation to the sufficiency and effectiveness of existing instruments in governing cyber security in their sectors. There are no directives or circulations specifically on cyber security or information security issued by sector leads to their agencies except in the case of MAMPU and the Central Bank of Malaysia. MAMPU has been issuing circulations to all government departments including those that are not in the CNII sectors.

During the interviews, all interviewees from sector leads have made reference to three main instruments provided by the NSC namely, firstly, NSC24, secondly, NCCMRCCP and thirdly, Cabinet Directive on ISMS implementation[13]. Findings from interviews highlighted several areas of concern at the sectoral level that are discussed in the next sub-sections.

6.4.4.1 Cyber Security Initiatives by Sector Leads

There have been initiatives conducted by the sector leads as reflected in this study. Based on the interviews conducted, sector leads have demonstrated their commitment in complying with the national directive NSC24. However, the commitment level varies from one sector to another.

In the government sector on security which is led by Organisation I, in addition to other national instruments, Organisation I has also issued security policies and directives related to information security for their sector. This included the ICT Security Policy issued in year 2010 which provides ICT security framework for the sector. Apart from that; Organisation I has deployed other governance instruments deployed in the government sector which Organisation I had been monitoring were namely, directive to perform cyber security posture assessment and another for the establishment of the Computer Emergency Response Team (CERT). In term of CNII agencies compliance of these instruments, Respondent1 explained:

> *Based on a survey conducted in year 2015 in 128 agencies in our sector, only 41.9% agencies were ISMS certified. Not only that, another mechanism is a directive issued by the Chief Secretary to the Government of Malaysia*

[13] NSC24 and Cabinet Directive on ISMS implementation and certification were deliberated in sub-section 1.2.2.2.

> *in year 2009 that all agencies in our sector were required to perform security posture assessment annually. However, based on recent measurement, there was only 41.9% comply with this circulation. We also issued a circulation in year 2006 for all agencies to establish CERT where only 57 complied. Thus, in order to ensure the effective implementation of these directives, we will work together with CyberSecurity Malaysia. Upon this implementation we will also perform a study on the impact of these implementation to ensure cyber security level is acceptable as required by our stakeholders.*

Respondent1 further added that although there were approximately 700 agencies in their sector, only 128 were listed as CNII organisations that encompassed all ministries, state secretaries and fronting agencies such state secretary offices and federal departments. Organisation I also performed security monitoring on individuals to avoid data leakage through deployment of data leakage prevention system. Respondent1 pointed out that in the pilot phase, about 1000 individuals were identified for installation of a mechanism or device agent at the individuals’ endpoint device to ensure data confidentiality was not leaked out.

In the case of the Organisation II, they initiated their own sector meetings and produced their own metrics of cyber security readiness. Organisation II also did consistent monitoring on the implementation of ISMS certification in accordance with the Malaysian Cabinet Directive where they have been updating their high level committee on the progress of the implementation four times every year.

Roles of regulators as defined by the NSC24 include ensuring agencies under their purview to comply with national policies and procedure. At the sector level, sector leads are also required to ensure their agencies comply with circulations or directives or statutory regulations or legislations meant for the sector. For example, for government agencies that belonged to more than one sector, apart from the directive or circulars issued by their sector lead, they were to abide by the government circulations issued by MAMPU.

In this study, for government agencies that were not directly governed by MAMPU, such as Organisation VII, circulations furnished by MAMPU to this organisation gave a signal that at some points, the directives had been effective. The interaction that took place between MAMPU and all government agencies had created the learning process for these organisation. Although Organisation VII had its own board of members that governed its activities, MAMPU still provided cyber security alerts and relevant information for Organisation VII to learn from the information shared. According to North (1994) the learning process of human beings (through time) could shape the way institutions evolved through interactions; where institutions created the rules and regulations while the organisations were the players. Using the game theoretic context, human interactions that occurred repeatedly was one of those discussed by North (1991) in stimulating cooperation. Other contributing factors included asymmetric information and large players in the group. Thus, regular and frequent communications and interactions between organisations and sector leads are capable of sustaining cooperative efforts within sectors.

Institutions such as enforcement agencies or regulatory bodies can exercise their roles in enforcing other economic agents such as organisations and the public in making the Internet a safer place for organisations to conduct their businesses and services. In a study related to safety at the workplace, one of the findings suggested that relevant institutions and government agencies should be involved proactively in enforcement roles and that institutional structure be strengthened in order to serve the industry better (Azizan Ramli, Mazlin Mokhtar, & Badhrulhisham Abdul Aziz, 2014).

In the healthcare sector, cyber security is also governed by the NSC and MAMPU as deliberated by Respondent3:

> *Only two institutions are being acknowledged in terms of regulating cyber security in our sector, first, the NSC through the National Cyber Coordination and Command Centre (NC4) and second, MAMPU through the Government Security Operation Centre (GSOC). We did deploy directives from MAMPU. When MAMPU requested us to develop security policies, we did. In terms of its implementation by the hospitals, Organisation III will do the follow-up with the team that performs the audit. When Organisation III developed security policies, we announced them to agencies under our purview for implementation that will fall under the responsibilities of the head of facilities. However, the heads of facilities tend to focus more on providing their core services, but not at all in terms of information security. Security requirements were not defined clearly. Our ministry did suggest to the facilities heads that security aspects should include ICT and should not be neglected. The head of facilities did cooperate on this matter.*

In the healthcare sector, security requirements were not defined clearly and it was clear that it was not given a top priority. Healthcare sector is a very critical sector as the impact of security breaches can affect human lives. It is prevalent that medical devices such as pacemaker and insulin pump were connected wirelessly and remotely for convenience purposes. However, a lack of security features in these devices could seriously pose threats to the patients. Not only can the patient’s information can be stolen, but patients could be remotely controlled if these devices were hacked. In this situation where Internet of Things (IoT) deployment is unavoidable, the sector lead should play a bigger role. Security requirements must be defined clearly and the usage of the connected medical devices should be monitored and controlled. For example, a relevant regulatory body can regulate products to have security features embedded to ensure users are not harmed by information that can be compromised especially on products that are related to healthcare devices. In the United States, the Food and Drug Administration (FDA) department provides recommendations for manufacturers to make medical devices more secure (U.S. Food and Drug Administration, 2014), following a finding by security researcher who managed to hack a medical device that has been commonly used in hospitals in the USA (Ree & Robertson, 2015). FDA also issued a warning letter to hospitals and patients that an infusion pump used to deliver a programmed amount of fluids into a patient's body could be vulnerable to cyberattacks; thus, the FDA encouraged for its discontinuation (U.S. Food and Drug Administration, 2015).

Any change in a business operating environment in all sectors should be reflected in their threat profile for the necessary countermeasures to be identified. Regulators for every sector should focus in identifying elements that subject to be regulated to ensure their sectors to be well-protected. For example, security requirements for medical devices. The spread of medical device that is handy through remote monitoring has prompted FDA to introduce guidelines in protecting the public who will be using the device (U.S. Food and Drug Administration, 2014). Through this directive, the industry is required to embed cyber security features in the product as early as in the design stage.

6.4.4.2 Confusion of Roles of Sector Leads

Although sector leads did share all relevant security information and directives to the agencies under their purview, there was still a grey area for these sector leads in playing their roles more effectively. This situation could be complex for sectors that have two sub-sectors. For example, in the financial sector; there are two sector leads; firstly, the Central Bank of Malaysia and; secondly, Organisation II. The Central Bank of Malaysia leads CNII organisations mainly from the private sectors such as commercial banks and financial institutions while Organisation II leads CNII organisations that are government entities. In the latter situation, agencies under the purview of Organisation II should be reporting their security incidents to Organisation II (being the sector lead) in accordance with the process as defined in the NCCMRCCP. However, this was not the case in their existing practice at the point when the interview was conducted.

In terms of daily ICT operational activities, agencies under Organisation II have been monitored by MAMPU through the Government Security Operations Centre (GSOC) where security sensors were deployed in their systems and were connected to the central systems monitored by MAMPU. As part of its normal day-to-day monitoring activities, MAMPU would notify affected agencies whenever cyber security anomalies were detected and these notifications were also sent to relevant sector leads. In other words, sector leads did not really play their roles as defined in NSC24[14].

In responding to the effectiveness of NSC24, Respondent2 observed that the existing directive was basically to ensure that they had a mechanism in place and for a sector lead to monitor their CNII agencies. However, their roles as sector leads became active only on occasions where there were cyber threats that can affect national security. In this situation Organisation II needs to monitor closely and receive updates from these agencies before escalating them to NSC at predetermined interval as defined in NCCMRCCP. This

[14] NSC 24 is the directive that provides terms of reference for managing cyber security crisis for CNII sectors in Malaysia. It was discussed in sub-section 1.2.2.2.

procedure states that cyber security incidents should be reported to respective sector lead. Respondent2 expressed her confusion over the overlapping roles of Organisation II as a sector lead, MAMPU and the NSC as given below:

> *If let's say MAMPU detects an intrusion in one of our agencies, so, they will alert our agency and at the same time we are also kept in the loop. We also monitor and make sure that actions are taken and the incident case is closed. And that is between us and MAMPU only. Yes, those are for the daily operations. But, when the NSC steps in and say there is a cyber security alert with potential national threat, then we will all start reporting to NSC.*

While being in these two different situations, Respondent2 stated that their role being sector leads were not clear under the existing practice with regards to reporting and she hoped that clarity in this matter would soon be provided.

6.4.4.3 Reporting Cyber Security Breaches

Not all sectors had their own cyber security incidents reporting structure. For example, in the healthcare sector, the incidents occurred in the public sector would ride on the Government Computer Emergency Response Team (GCERT) establishment. GCERT is a central reporting centre for cyber security incidents reporting for the government sector. However, the incidents reporting was meant for government agencies only. There was an absence of this establishment for the private hospitals in this sector as stated by Respondent3:

> *In terms of information security implementation in private sector, if ICT department exists in an agency, I assume that they should have these type of activities. ISMS covers assets protection which are under the responsibilities of CIO. In the case of National Heart Institute, they have their CIO to ensure the implementation. They even adopted the ISMS*

> *standard. But, the question is if incidents happened whether they had to report or not. Most probably, if it happened, they would try to resolve the incidents themselves. However, Organisation III do not know what would happen in the private sector as there was an absence of a centre to report cyber security breaches that originated from the private hospital, unlike public hospitals. If it happens in the public hospitals, it should not be a problem since MAMPU will know the number of incidents that have occurred when the incidents were reported to GCERT.*

6.4.4.4 Constraints of Resources

Financial capabilities vary from one sector another. There was a constraint of resources for adhering to national policy instruments. Respondent3 stated:

> *In terms of enforcement, the NSC just issued the directives, but did not package with the financial assistance. Not all hospitals have security technologies deployed and security experts. Not all hospitals have security technologies deployed although they should have had the security perimeters installed such as firewall or IPS and monitor pendrive or wi-fi on the internal threats. As for cyber security experts, not all agencies have the required competencies. If they do not have, Organisation III will assist.*

The healthcare is not the only sector that has security budget constraints. As highlighted by Respondent2, due to budget constraints they were deprived to be at the field to do the actual monitoring of the systems and security events for their sector. Respondent2 explained:

> *Well…I think whether we like it or not, we have to do it. They will audit the compliance. So you just need to implement it. You have to make do whatever you have...and you have to build up the expertise in those areas which you think your people are lacking of.*

This is particularly true with the increasing sophisticated attacks, not only the government, but other CNII sectors should be able to invest in security particularly related to human aspects such as capacity building, training of the workforce and awareness programmes. Respondent8 admitted on the challenges of resources where they plan to pool them together and train them, where they can later train others.

6.4.4.5 Technical Information Sharing at Sector Level

Information sharing can also be seen as a mechanism by organisations to assist other organisations in preventing security breaches especially to organisations that have constraints in budget and resources especially when they are in a similar sector. Respondent6 suggested that it is important for information related to cyber security threats, vulnerabilities and incidents to be shared within the sector to understand the current threats and vulnerabilities that were similar within the sector, so they could share the same preventive and corrective measures when cyber security incidents occurred. By sharing these critical technical information, all organisations in the sector can have better solutions and would be able to resolve any security issues faster. This is supported by Ahmad, Hadgkiss, and Ruighaver (2012) where sharing of information is significant for organisations in managing information security incidents should they occur and to also learn lessons from others in order to prevent similar security incidents from occuring in the future. For example, organisations that have deployed intensive or sophisticated threats detection tools can share the information captured by these tools to other organisations that have no such tools in place. By sharing this information, relevant actions can be implemented to deter possible attacks and if it happens, the duration to contain and identify the root cause of the security breach can be minimised. This is supported by Gordon, Loeb, and Lucyshyn (2003, p.472) that when firms share information on security activities, there will be less expenses incurred by each firm compared to when information sharing is absence, gradually achieving same level of security amongst them with a smaller cost to each firm. Thus, for technical information sharing to be shared amongst organisations in specific sector, institutional role is observed to be important in coordinating and managing this effort.

6.4.5 Governing Cyber Security at the National Level

Although the quantitative results show that governing cyber security at the national level for the CNII sectors were significant, the findings of the interview provided some insights that were important for consideration.

6.4.5.1 Review of National Cyber Security Policy

The study of National Cyber Security Policy (NCSP) was conducted by MOSTI in 2005 and introduced for implementation soon after. The ownership was later transferred from MOSTI to NSC in 2011 due to NSC for being responsible on issues related to national security (Shamir b. Hashim, 2017). However, this policy has never been reviewed since its inception in 2006. Thus, this study observes that it is timely for the policy to be reviewed to ensure it is relevant to the current cyber ecosystem and threats. Although some security initiatives of thrusts are still on-going, cyber threats have become very dominants in almost all organisations and cyberattacks have become very sophisticated. For example, technologies and devices related to IoT environment are prevalent in meeting users' demand and convenience. Failure to govern sectors that have direct public interest such as healthcare services in deploying medical devices without putting serious efforts on security aspects of it, the consequences can be huge not only to that particular sector, but also to the government in general. In responding to this matter, Respondent8 agreed that the policy should be reviewed and in the planning stage. Thus, this requires immediate attention for a review.

6.4.5.2 Incident Reporting Between Organisation with Sectoral and National Levels

Although there is a national incident reporting procedure is in place, it is observed that there are inconsistencies in the procedure within different sectors. The possible reason is due to the absence of physical establishment of the coordination centre which is known as National Cyber Coordination and Command Centre (NC4). According to NSC 24 directive, the command centre was meant to be the centre that does not only provide coordination amongst organisations in CNII sectors, but also technical assistance in resolving cyber security incidents in peace time and crisis time.

However, in practice this is not happening. Based on the National Cyber Crisis Management Response, Communication and Coordination Procedure (NCCMRCCP), for incidents occurred in a CNII sector, the affected organisations need to report these incidents to their sector lead. If their sector lead was not able to resolve the problem, the problem should be escalated to NSC through the coordination of NC4. Respondent2 stated:

> *Currently, we are reporting to MAMPU because MAMPU monitors all the security events in the government agencies security and we are also covered under the Malaysian Government Security Operation Centre (GSOC), so when there is a security event…they will alert us.., but according to CNII setup, we are supposed to report to NSC. Since at the moment there is no NC4, unless NC4 takes over, then we will report to NC4. So, we don't need to report to MAMPU unless MAMPU say there is no need for us to report to them. But, now when they say that they detect security breaches in our sector, we still need to fill-up the form and report to them (MAMPU), so I don't know how is their coordination with NSC.*

Due to the current practice of incident reporting that does not adhere to NCCM Procedure, this creates confusion. When there is an incident happens that could potentially affect the nation, the affected organisations need to report and update the incident in two different forms; one using the form provided by MAMPU and another furnished by the NSC. According to Respondent2, while responding to security incidents; reporting and updating the two different entities (MAMPU and the NSC) using two different forms is not efficient. This argument is also supported by Respondent1 and Respondent3. This is very true as cyber incidents can spread so fast. Although NC4 was established in early 2017, it was not fully functional yet. Thus, NC4 needs to be fully functional as soon as possible as this coordination centre is not only needed during crisis, but also during peace time in accordance with terms defined in NSC24.

6.4.5.3 National Cyber Drill and Cooperation

One of the means to ensure the preparedness of CNII organisations in responding to cyber security attacks is through national cyber exercise that is defined under policy thrust 7. Not only to meet the objective in coordinating CNII sectors when there are cyber security incidents, but also to foster collaboration between the public and private sectors. This collaborative efforts are designed under the policy thrust 7 of NCSP. The national cyber drill is designed taking into account the latest global attacks and incidents where the scenario was simulated to participating sectors. Since the inception of National Cyber Crisis Management Response, Communication and Coordination Procedure in 2008, there has been six cyber drills conducted where the sixth was conducted in January 2017 (Bhunia, 2017). The drills were conducted with the purpose to gauge the readiness of agencies in CNII sectors in terms of technical skills and competencies and familiarity of CNII sectors on reporting and escalation of incidents to relevant stakeholders.

The drills have somewhat improved not only coordination at both sector and national levels, but also the competency level of organisations in responding to attacks which requires cooperation at three levels; organisations, sectoral and national. In preparation for the national cyber drill, the NSC will organise several workshops where participating organisations were required to attend. In meeting the objectives of the drill, cooperation from participating organisations and sector leads were required from the moment the drill was announced until the drill event was over. Participating organisations had to ensure the right representatives attended these sessions to capture the course of actions to be done in their organisations in preparation for the drill. It is also important for the same representatives to attend the sessions to ensure the continuity of handling this event, so the organisations could prepare the drill smoothly.

As argued by Respondent2 and Respondent6, although the national procedure team, the NC4 was meant for both during peace time and crisis, the procedure was only applied during cyber drill and when there was possible crisis to be detected. Otherwise, it was not applicable in peace time because the NC4 team was not fully functional yet. In fact, it is still in its transition phase in providing its defined role.

6.4.5.4 Malaysian Cabinet Directive on ISMS Implementation and Certification

All interviewees made reference to the ISMS implementation as per Cabinet directive[15] . ISMS has been acknowledged as a practical and holistic approach in governing information security worldwide. The directive approved by the Malaysian cabinet institutionalised organisations in inculcating risk-based decisions for their employees to perform their tasks while ensuring information were protected. The adoption of organisations to implement and practice international standard such as ISMS in their organisation supported the institutional theory by North (1991) that institutions were rules of the games and organisations were the players. While MAMPU in this context being

[15] The cabinet's decision was obtained in year 2009 in defining the rules for CNII organisations to implement ISMS and obtain certification within three years of its issuance. More details can be found in sub-section 1.2.2.2.

the regulator of the government sector, they cascaded down this directive to all agencies under their purview. But, not all government agencies adhere to their circulation especially to those that have their own governance set-up. In this study, although Organisation II is a government funded entity, their independence from MAMPU does not require them to adhere whatever proposed by MAMPU. At this point, it is at the discretion of their governance board to implement circulations issued by MAMPU. According to Respondent7, not all circulations related to information security will be adopted by their top management. She further highlighted a lack of budget that had caused the constraints of certain security deployment in Organisation II.

6.5 Summary

Using an ordinal logistic regression analysis, document reviews and interviews, this chapter shows that cyber security governance instruments deployment are more significant at both organizational and national levels rather than at sectoral level. Organisations were transformed into risk averse organisations since the cabinet directive was issued for all CNII sectors to implement ISMS and get certified accordingly. Through this transformation, CNII organisations became more alert on uncertainties in cyber security which their organisations were facing. Since previous studies argued that people factor in information security is the weakest link, the three significant governance instruments deployed in organizational level were all people-centric namely, established security governance structure, top management in leading security and information security audit. These were internalized through policy directives at both national and sectoral levels.

The institutional change demanded information security structure to be established in providing a clear platform in deliberating cyber security matters together with defined roles and responsibilities. This has made more organisations chose to appoint someone from the top management level to lead security in organisations. However, apart from having leadership qualities, the appointed person should also have relevant cyber security skills and competence to ensure cyber matters are adequately addressed. Having someone with high ranking officer such as a CIO or CISO in organisations is observed as an approach to address the pressing needs of top management in leading security in organisations. However, if security responsibilities are considered as an extra role, CIOs in the government sectors would not be able to understand the whole security environment within and outside the organisation; thus defeats the purpose of their appointment.

The role of information security audit was also seen as an effective tool in checking how employees participate and cooperate in adhering to security requirements. Although several literature claimed that security compliance do not justify for security breaches not to occur, this study do not wish to guarantee that breaches will not occur. Instead this study suggests for cooperative measures to be deployed in boosting self-belonging while creating distance for free riding attitudes in employees.

Roles of sector leads are observed to be important in instilling interaction for organisations under their purview to perform in security aspects. However, unclear roles deter sector leads in performing their roles effectively. Without a full function of the coordination centre for CNII organisations to report cyber security incidents, it creates uncertainties on the directives of cyber security for these sectors.

This study has identified that there is a lack of platform in sharing technical security information for organisations to understand the current cyber security threats and issues pertaining to every sector. Thus, this study proposes for an information sharing platform to be established within each sector as to capture common cyber security threats, vulnerabilities and incidents pertaining to each sector. Similarly, to understand the global issues, a centralised information sharing centre should also be established accordingly.

CHAPTER 7: CONCLUSIONS AND IMPLICATION

7.1 Introduction

Previous studies on cyber security compliance had informed us that very little work has been done on the role of cooperation on cyber security compliance amongst organisations. Drawing from various theories namely, public goods, cooperation, theory of planned behaviour, institutional and power distance, this study is sought not only to fill the gaps, but to make significant contributions to theory and policy to raise cyber security compliance. Being the first to apply public goods theory and cooperation in cyber security compliance, the findings offer novel extensions to both theory and policy. This study also offers methodological contribution in relation to how critical qualitative approach is crucial in providing insights to conclude a study. The interviews conducted at every governance level were able to deliberate the real issues on the ground. They were not only capable to support the quantitative findings, but also to offer an in-depth analyses on the subject to be studied, which are the effectiveness of cyber governance instruments implemented at organisational, sectoral and national levels.

7.2 Synthesis of Research

This thesis began by looking at problem in the rise of cyber security breaches (Ponemon, 2017; Thales, 2018) despite of strengthening of security technologies and huge budget allocation for protection measures by some organisations (Riley et al., 2014; Thales, 2018). The problem of cyber security is due to its non-excludable characteristic being a public good (Johansen, 1977) where no one can be excluded from benefiting the good although they do not contribute to it. This free riding effect or also known as the "failure of collective actions" (Deneulin & Townsend, 2007; Stigler, 1974) which can be detected through lack of cooperation (Burdett, 2003; Itoh, 1992) and group size effects (Albanese & Van Fleet, 1985). The people issue being the weakest link was integrated with the lack of cooperative behaviour (derived from non-excludable aspect of public good) which led to the problematisation of this study. Thus, factors to motivate cooperation were identified as an alternative approach to mend this situation. Apart from theory of public good (Hardin, 1968; Rosenzweig, 2012), theory of cooperation (Axelrod, 1984; Killingback & Doebeli, 2002) and institution (DiMaggio & Powell, 1983; North, 1991, 1994) were also studied in addressing the issue.

By looking at the factors that motivate behavioural intention of employees to cooperate, which, in turns affect cooperation in achieving cyber security compliance, this study addressed the research question 1. Using Theory of Planned Behaviour (Ajzen, 1991), this study analysed security awareness (attitude), security role (subjective norm) and security technical capabilities (perceived behavioural control) being internal factors in motivating ITC. An external factor identified in predicting ITC was institutional role.

Adopting quantitative approach, the collected data was later analysed using BLR analytical method in predicting whether employees have the intention to cooperate in achieving security compliance as shown in model 1. The analysis found that security awareness (Albrechtsen, 2007; Bresz, 2004; Safa et al., 2015; Siponen, 2000), institutional role and security roles at top management and middle management levels transformed the behavioural change of employees to cooperate. These two platforms are able to create sense of belongingness among employees to meet common organisational objectives through positive interactions between them. A distinct feature identified is that communication (Adams & Sasse, 1999; Mohammed, Mariani, & Mohammed, 2015; Sally, 1995) through repeated interactions (Cooper, 2006; Flowerday & Von Solms, 2006) between these individuals not only can induce cooperation but deter free riding behaviour (Isaac & Walker, 1988), which can be found through exposure to frequent and consistent awareness programmes held in organisations. The role of top management

(Birken, Lee, & Weiner, 2012; Floyd & Wooldridge, 1994; Knapp et al., 2006; Puhakainen & Siponen, 2010) and middle management (Birken, Lee, & Weiner, 2012; Floyd & Wooldridge, 1994) should not be underestimated in earning the trust of employees in providing their cooperation for performing the required tasks. The role of institutions (North, 1991) is also observed as critical in internalisation of national policy directives through sector leads.

For model 2, using the same BLR analytical method, ITC was found to be significantly predicted cooperation. This support previous studies by (Jeffries & Becker, 2008; Pahnila, Siponen, & Mahmood, 2007; Siponen, Mahmood, & Pahnila, 2014) where behavioural intentions were the precursor to actual behaviour.

Using quantitative data and KHB approach (Breen, Karlson, & Holm, 2013; Karlson & Holm, 2011), the intervention of cooperative behaviour of organisational practices towards CSC was investigated in answering research question two. The indirect effects of cooperation on three selected security organisational practices towards CSC were studied, namely, top management commitment (TMC), structured security practices (SSP) and security investment (SI). The findings show that TMC and SSP have both direct and indirect effects of cooperation in their relationship with CSC. Drawing on institutional isomorphism (DiMaggio & Powell, 1983), the findings also show how organisations' inclination towards risk-averse conduct was influenced by significant role of institutions played by sector leads and the central authority. Uncertainties in cyber ecosystem encourage organisations to imitate other organisation's good practices to minimise their risks.

Security processes naturally involve tasks to be performed interdependently across the business units in organisation. The situation can be difficult when security issues become more complex; thus requires a structured approach for a smooth cooperation in addressing security issues proactively and reactively. As argued by Mulej, Rebernik, and Bradac (2006), any complex problems cannot be resolved by individuals due to limitations of human capabilities except cooperation. Thus, having proactive and reactive security processes integrated into a security processes framework provides a holistic approach for employees to perform their tasks while not ignoring security threats and risks (Maslina Daud et al., 2018). However, the study found that there is no indirect effect of cooperation on SI although SI contributed to CSC. Making both investments on technologies and humans to raise competencies work hand in hand that help complement each other's role.

In answering research question 3, a mixed methodology was applied to evaluate the effectiveness of cyber security governance instruments implemented at three levels namely, organisational, sectoral and national levels in achieving CSC. In addressing this research question, apart from public good theory the institutional theory were also examined to associate the instruments' effectiveness with CSC. For the quantitative data, OLR analytical method was used to perform the data analysis due to its ordered dependent variable. For the qualitative part, interviews were carried out at the three levels involving eight (8) organisations to support the quantitative data for conformance and clarity purposes.

The OLR findings showed that cyber security governance instruments deployed at both organisational and national levels have been effective in achieving CSC in comparison to those at sectoral level. Supported by the interviews conducted, the findings clearly showed the influence of institutions on the role of sector leads as policy implementers. However, although sector leads were given the power to implement the policies defined by the central authority, the implementation of it is not clear. It creates confusion especially for agencies that are in sectors that overlap with the government sector. Using cyber drills experienced by sector leads, they saw their roles as defined in NSC24 came to force only when there were cyber threats that could potentially turn into a crisis that could affect the nation. Only during this period where the reporting structure as defined in NSC24 and NCCMRCCP came into effect where CNII organisations reported and furnished updates to sector leads, then sector leads reported to NSC. In other words, during peace time on the day to day operations, reporting structure seems to be dormant. As declared in NSC24, the existence of the NC4 is to provide better picture for the reporting of future incidents and coordination of agencies and sector leads together with NSC.

It is evident from this study that, the non-excludable aspect of cyber security being a public good require collective efforts that can promote behavioural intention in achieving CSC. Consistent security awareness programmes embedded with effective communications have somehow instilled a sense of belongingness and close association among employees to cooperate in achieving common security goals in organisations. The indirect effects of cooperation in certain organizational practices towards CSC offers a critical discovery that was not offered in previous compliance studies, thus makes this study different from them. As argued by Hardin (1968) where regulation is needed in governing public good to resolve the public good problem, this study shows how role of institutions matter in internalizing national policy directives through sector leads. Although the findings found some weaknesses in the implementation, they can be overcome by policy review which is currently underway. Having presented these findings, this study turns to drawing implications for theories that in the next sections.

7.3 Implications for Theory

Chapters 4, 5 and 6 examined the issues in the research questions, and the relevant theories, namely, public goods, collective action, free riders, cooperation, institutional theory and power distance. Public goods are associated with non-rivalrous and non-excludable characteristics. The latter characteristic contributes to free riding attitude by members in a group. Previous scholars suggests that the lack of cooperation among group members who are opportunistic may result in them taking advantage of the benefits of public goods without contributing it. In this situation, members should work collectively in sharing public goods.

This research provides several crucial theoretical implications. The analysis of motivating factors for employees to cooperate contributes new insights into how cooperation results in the improvement to managing public goods. The examination of intervention of cooperation in selected organisational practices provides positive implications to management and security processes. Finally, the interviews conducted contributed a profound understanding role of institutions in strengthening cyber security compliance in the three hierarchical governance levels; organisational, sectoral and national.

Power distance measures the extent to which subordinates who are less powerful members in organisations or institutions accept the unequal power distribution and submit to those who have authority.

The results provide evidence of people's opportunism to take advantage of the non-excludable aspects of public goods, such as cyber security. In a situation where people cannot be excluded from free riding in the consumption of such goods, the alternative is to foster cooperation to prevent its abuse. The results also show that security awareness programmes embedded in effective communication systems also function as channels for employees to interact with one another to strengthen cooperation. Security awareness is critical to keep the focus of employees over the need to beware and to police cyber security issues. Constant interactions between middle management (who are the implementers of cyber security programmes) and employees can induce cooperative behaviour in meeting common security objectives as defined by the organisations. Such interactions help employees build a sense of belongingness in contributing towards shared and collective beneficial security compliance networks in organisations. Sense of belongingness created can overpower self-interest. Efforts to build cooperation can ward off opportunists from hacking cyber security platforms. While free riding is both unavoidable and is often desirable, cooperation can prevent such avenues from being abused. Interestingly, the findings also conformed the inverse association where the larger the group is the less cooperation obtained, thus contributing to free riding activities.

This study supports the cooperation theory. In groups that are non-related (who do not have genetic relation), such as employees in organisations, social embeddedness instilled through interactions (from security awareness and effective communication), motivates reciprocity that escalates to altruistic behaviour for the achievement of better cyber security compliance in organisations.

The non-excludable characteristic of cyber security and cooperation through collective efforts by employees provides a synergy, which results security compliance. The evidence offers a new perspective in understanding behavioural compliance where it can complement existing studies from the lense of cyber security being a public good. The problem of cyber security that stems from the non-excludability aspect of public goods can be overcome by encouraging employees to cooperate. Thus, it provides an avenue to assess behavioural compliance from a different approach. This study also supports both theories where cooperative efforts can lead to acceptable behaviour through collective actions occurring in specific organisational practices, such as TMC and SSP in meeting common goals. Our results support Rasiah's (2011) argument where cooperation mediates organisational practices in achieving security compliance. In a situation where people cannot be excluded from consuming such goods (in this context is cyber security), this can be an invitation for opportunists to benefit from the secured operating environment without contributing. This is a significant contribution in the public good theory where non-excludability is unavoidable, cooperation could be the solution to cyber security problem. This study also supports previous security researchers who called for information security issue to be explored from the micro-economics perspective (Anderson, 2001; Schneier, 2007).

These results also show the importance of an institutional role in shaping organisational practices to achieve cyber security compliance. Using the definition of institutions and learning by (North, 1991); North (1994), this study demonstrates the importance of institutions in transforming CNII organisations to risk averse organisations. A blend of institutions emanating from socioeconomics origin targeted at moulding and shaping the conduct of individuals, firms and organisations collectively help stimulate cyber security compliance (Rasiah, 2011). This finding is significant in prepare for future attacks by complying with directives through guiding principles formulated in the directives. The issuance of government directives to implement the ISMS and provision of guiding principles help to promote better security management. The adoption of organisations to implement and practice international standard such as ISMS in their organisation support the institutional theory where institutions are rules of the games, individuals, firms and organisations are the players.

It should also been emphasized that cooperative efforts are needed to implement security processes to provide an environment that encourages consistent positive interaction and collective action among employees, so as to deter negative behaviour by opportunists. Supported by Ramamoorthy and Flood (2004), in an environment where tasks interdependence is high, individualists tend to move away from their own objectives, but move closer to the group by being helpful and cooperative. Wageman (1995), also suggested that in a complex operating environment where interdependencies are high, often consistent and high level of interactions are required. Thus, security processes should be structured, documented and communicated to allow employees to perform their tasks in a collective manner. The adoption of the ISMS reflects the needs of standardised, structured, documented and continual improvement that benefits the whole organisation. Although the ISMS is mainly observed as a process approach, it provides a holistic security practice that requires both proactive and reactive aspects derived in the form of security controls as the outcome of risk assessment exercise. Learning experiences from both approaches and rehearsing and responding to security incidents will allow organisations to stay resilient to the fast changing threats in the cyber security ecosystem. For security processes to be effectively deployed, relevant skills and competency should be developed and accordingly enhanced to ensure they are relevant. Thus, both proactive and reactive security processes provide the necessary platform for interactions among employees. This does not only allow them to perform their tasks within their department but also at the interdepartmental level in a collective manner, that deters opportunistic behaviour in complying with security policies, procedures and other requirements.

The results of this study shows the importance of institutions in transforming organisations from non-risk to risk based organisations through the ISMS directive. Through the proposed integrated cyber security processes framework, organisations can become more resilient through the deployment of proactive and reactive approaches. The framework also describes cooperation amongst employees' that can be obtained throughout the described security processes in achieving security compliance. To achieve security compliance without excluding opportunists, emphasis on cooperative behaviour is fundamental where social embeddedness among a group employees can be instilled through security processes as they perform their tasks.

The results of this study shows how institutions influence CNII organisations in transforming them from uncertainty into risk averse organisations. Institutional roles through cabinet directive to implement ISMS suggests how institutions have successfully set the game (practice) for organisations in CNII sectors to stay alert on the threats to become more resilient. The roles of institutions are further emphasized through monitoring by sector leads throughout its implementation. The evidence of this study suggest interactions between sector leads (as institutions) and organisations are capable to institutionalise organisations in shaping them into becoming risk averse organisations. Learning that is instilled through security awareness programmes, communications on security information, information sharing and continual improvement through ISMS implementation supports North's (1994) theory that learning is fundamental for organisation to survive. Through continuous learning, organisations not only build competencies of employees in organisations, but also provide relevant security knowledge to employees in building resiliency organisations by staying alert, responding fast and minimizing adverse effects that can eventually create sustainability in organisations. It is also critical to take the direction of (Veblen, 1915), (Nelson & Winter, 1982) and (Rasiah, 2011) that a blend of socioeconomic institutions collectively rather than supply market institutions alone are critical in moulding the conduct of individuals, firms and organisations to promote cooperation.

Institutional change has also transformed the roles of NSC to balance the interests of public and private sectors in handling cyber security aspects through cyber drill exercises. These exercises provide a learning curve for CNII organisations in building competencies and skills in resolving cyber security breaches and mitigating impacts of the breaches. Cooperation achieved during the drills through consistent interactions between CNII agencies and sector leads, the latter with NC4 before and during the drills. In this exercise, the roles of NC4 are crucial in providing coordinating platform for all players to cooperate in accordance to the national procedure. Although role of NC4 are documented in the cyber security governance structure in NSC24, its roles are being observed to exist only during these exercises. This study is also supporting cooperation theory where the institutional role helps to motivate cooperation in its ecosystem. The presence of NSC in organising and executing these drills drive cooperative behaviour not only between agencies with their respective sector leads, but also amongst agencies within sectors. During the exercise, CNII have been cooperative in sharing security information in mitigating threats as defined by the scenario of the exercise.

This study also enhances the power distance theory suggested by Hofstede (1980). Using this study as an example where Malaysia is the country that has the highest power distance, additional criteria to be defined for those who are in senior management in driving cyber security implementation in organisations. These criteria can include security background, knowledge, experience, strategy and relevant security certification the top management has to possess. Having a security leader who has these criteria will passionately lead organisation towards a security culture organisation, which can ensure the production of positive implications and benefit from this cultural domain. The evidence of top management’s security role in contributing towards behavioural intention to cooperate shows how information security should be prioritized in organisations.

7.4 Implications for Policy

The examination of governance instruments at the three levels, organisational, sectoral and national through quantitative study and supported by interviews suggest that although related national policies are in place, little findings can help strengthen monitoring and implementation. Thus, this study proposes four main policy implications.

7.4.1 Revision of National Cyber Security Policy

Three governance instruments were discussed in this study to regulate cyber security in CNII sectors, namely: NCSP, NSC Directive No 24, NCCMP and the Malaysian Cabinet directive. Based on the evidence, the availability of these instruments do not reflect the effectiveness of their implementation. Although Organisation VIII (the central authority) had programmes in place to introduce the directive for implementation, very little promotional efforts and consistent monitoring of the implementation has been done. Without these efforts and programmes, the effectiveness of implementation of these directives will not be materialized. In addition, the national policy (NCSP) that was adopted in 2006 is timely needs review in accordance with the latest developments forms of cyber security threats and risks. This is to ensure that the policy stay relevant with the current cyber security ecosystem.

The evidence also shows that NSC is the key agent responsible for cyber security in CNII sectors. The request from NSC for SLs to monitor their sector and provide situational update to them only happens when there are potential threats to the nation. This request reflects that the process as defined in the NCCMP. In monitoring the situation, SLs need to request update and assess the impact from time to time as determined in the procedure. As for some government agencies where ICT budget is allocated by MAMPU, the reporting process is not aligned with what is defined in the national procedure during the peace time. In times of security stability, any security threats hitting their systems should be notified by MAMPU directly to the government agencies.

It is also proposed for the scope of this policy to be extended to two other critical segments of the nation; i.e., Small and Medium Enterprises (SME) and the public. The rationale is that SMEs are in a sector where business segments use online transactions to take advantage of the convenient and cheaper marketing expenses afforded by such a mechanism. The latter is critical due to quick and easy propagation of malware infection when users have more than one device particularly through the prevalence of IoT.

7.4.2 Security Leadership Criteria

Although there are no specific cyber security organisational chart were used during the interviews, elements such as top management in driving security and committees are described as part of governing security by some organisations. These suggests that appropriate governance has been in place. As for the government sector, creating CIO as a dedicated post instead of managers assuming just additional roles can create a big impact. Thus, this study is proposing adaptive governance in governing cyber security system in organisations taking into considerations the current cyber environmental and ecosystem where organisations adapt existing organizational practices that can create a sustainable cyber security ecosystem. One of the approaches to move towards adaptive governance is to create the CIO's position in the government sector as a dedicated post ensure that there is focused governance. In addition, in leading security, CIOs should be sufficiently equipped with information security experiences to ensure that security matters are appropriately steered. Described as adaptive governance, the governing instruments in organisations should be sensitive to current environmental aspects where cyber security ecosystem should also follow suit the other social ecosystems. Thus, the national security policy should require CIOs in the government sector as well as in other sectors to be competent and well-equipped with security knowledge and experiences where security becomes their primary task for the organisation.

7.4.3 Sectoral Threat Profile

Governance instruments implemented that cut across all sectors although cyber threats might not be the same for all sectors due to the nature of systems used. Thus, creating own threat profiles for every sector helps sectors to stay alert on impending threats and potential impacts the threats might have on their sectors. By profiling threats relevant to each sector, sector lead can analyse changes in threats in accordance with the changing environment and take quick countermeasures of the changes to adapt to the current threat scenario. Sector leads should lead the adaptation of changes that should be cascaded down to all agencies under their purview. A consistent update on threat profiles is significant so that sector leads can consistently assess regulatory aspects to be imposed in their sectors through issuance of directives or guidelines to be adhered to by stakeholders of their sectors. Thus, the national security policy shall require all CNII sectors to establish their own sector threat profiles, where these sectors shall internalize the same for organisations under their purview.

7.4.4 Sectoral CERT Operations and Technical Information Sharing

The insignificant results of governing cyber security at sectoral level suggest that the role of sector leads and existing instruments need to be revisited to ensure their relevance today. Technical information of cyber security threats, vulnerabilities and incidents within the same sector are crucial to be shared. These information not only helps other organisations in the sector to prevent similar security breaches from happening, but also, helps those that do not have security tools in place to thwart impending security attacks. Thus, an official platform to share these information at the sector level is crucial. Platforms to share these information can vary. One of the platforms is through CERT where incidents are be being reported to and managed. However, most CERTs at the sector level are functioning as an established platform to monitor incidents progress only. Thus, this study proposes for CERT at the sector level to become a platform for technical information sharing, which will be able to stay alert on the threats and vulnerabilities associated with their sector. CERT for each sector can also leverage its sector threat so that its profile is updated from time to time depending on the current threats and vulnerabilities. Thus, having sector threats profile with consistent updates is one of the aspects of adaptive governance, which is proposed in this study for governing cyber security at sector level.

Although not all sector leads have established their own dedicated CERT teams to manage cyber security incidents due to scarce of resources, sector leads may consider establishing a virtual CERT. This means that the team is established with members from various departments using terms of appropriately defined references. The team members may not be wholly dedicated in running this team, but it is formed as and when required, especially when an incident occurs that could potentially affect the sector or nation. However, incident management procedures need to be developed and implemented; so members in the team are familiar with what to do as and when required. The sector CERT team can also become the platform for exchange and sharing of technical information.

In the United States, an executive order was issued by its President in February 2015, where information sharing between the industry and the government and within the industry is to be built upon the framework of National Institute of Standards and Technology (NIST) to communicate cyber security issues effectively (The White House, 2015). The order is to be deployed through collaboration of the said entities where Information Sharing and Analysis Organisations are to be established and information is to be shared voluntarily. Therefore, national security policy shall require each sector lead to establish its own CERT and a technical sharing platform for the benefits of organisations under their purview.

7.5 Implications for Practice

This research provides some implications for practices based on examinations and analysis conducted to answer the three research questions. Thus, this study proposes two recommendations for consideration. Since cyber security is a global issue, organisations worldwide were also sought to consider the deployment of these recommendations.

7.5.1 Extension of Scope for ISMS Implementation

This study proposes for organisations to extend the scope for ISMS implementation beyond ICT department, which was raised by several respondents (Organisation I and Organisation VII) who are at the middle management level. By not extending it, there is a tendency for relevant risks and threats to be underestimated, and hence, the necessary countermeasures may be overlooked. Thus, this study proposes for organisations to extend the scope of ISMS implementation to cover critical business operations. Since the evidence shows that the middle management interacts intensely with employees on security policies and procedure implementation, it is wise to leverage their strength in extending ISMS scope of implementation in CNII organisations. This study also proposes for CNII organisations to establish threat profiles. Having a threat profile provides a means to prioritize threats and enables the mobilization of capabilities to respond to them effectively by mapping the threats with the source of the threats or events. Sharing these profiles with other organisations can also help identify security solutions in a more effective, predictive and cheaper way.

7.5.2 Integrated Cyber Security Processes Framework

Finally, this study proposes for an integrated security processes framework to be adopted in organisations as it is not only protects cyber security in organisations, but also builds security resiliency through proactive and reactive approaches. The above discussion highlights tasks that are interdependent in prominent security processes in organisations that requires cooperation at some points. Imagine this scenario, when incident occurs, in identifying the root causes of the incident, the digital evidence must be acquired and preserved accordingly. In this context, the process requires tasks that are interdependent, and should be based on a different skillset that is in line with suggestions of Van Der Vegt, Emans, and Van De Vliert (1999).

Due to the lack of integrated security processes, this study proposes a framework that take into consideration proactive and reactive processes to ensure resiliency of organisations against cyber security breaches. These processes involve two factors that fits the definition of task interdependence as suggested by Guzzo and Shea (1992). Firstly, the need for a certain degree of interactions with other members in the organisation in completing each other's task is pertinent to finish the whole task (which is to achieve information security) and secondly, the need to share resources in meeting the objective. All processes described in this framework require cooperation among all employees to ensure cyber security is managed as the highest priority. There are three main processes that build the foundation of the framework, namely, information security management, business continuity management and incident management whilst another two that are similarly critical to be implemented are security vulnerability assessment and security events monitoring. The proposed framework is presented in Figure 7.1.

To use ISMS as the foundation in managing information security in organisations, it requires the fundamental process of risk assessment exercise. The process assesses threats and its associated vulnerabilities, and assesses risks related to information security. In mitigating the risks, security controls are identified as the outcome of the risk assessment exercise, deployed and eventually measured to assess its effectiveness.

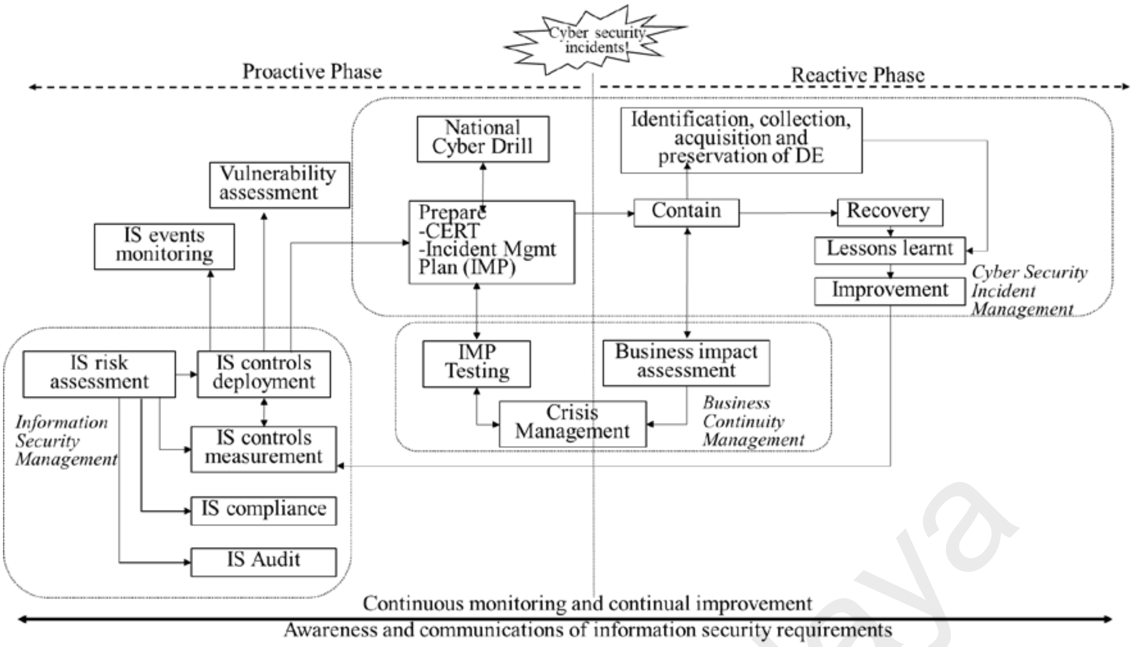

Cyber security incidents!
Proactive Phase
Reactive Phase
National Cyber Drill
Identification, collection, acquisition and preservation of DE
Vulnerability assessment
Prepare -CERT -Incident Mgmt Plan (IMP)
Contain
Recovery
IS events monitoring
Lessons learnt
Improvement
Cyber Security Incident Management
IS risk assessment
IS controls deployment
IMP Testing
Business impact assessment
Crisis Management
Business Continuity Management
Information Security Management
IS controls measurement
IS compliance
IS Audit
Continuous monitoring and continual improvement
Awareness and communications of information security requirements

Figure 7.1: Integrated Cyber Security Processes Framework
Source: Author

One of the common security controls required is the establishment of an incident management procedure (IMP) together with its CERT team. Capabilities of the team and familiarity of team members on how to respond to security incidents using the IMP should be regularly tested. The testing of IMP and CERT should be done not only at the organisational level, but also at the sectoral and national levels. Under the NSC Directive No 24, CNII organisations are required to participate in the cyber drill through National Cyber Crisis Management Procedure (NCCMP) where cyber security incidents are managed and coordinated across all CNII sectors nationwide (Digital News Asia, 2013). Thus, whilst developing and enhancing the IMP, the integration of the organisational IMP with the NCCMP should be considered to smoothen responses and cooperation with respective sector leads and NSC.

In the event of cyber security breach, the IMP should be invoked where the CERT should try its best to contain the incident from spreading to the rest of their corporate network. At this juncture, the BCM team should be activated to assess the impact of the security incidents to the organisation. This information is to be consistently shared and communicated with BCM, CERT and crisis management team to ensure that actions are taken to control the situation and to avoid the incident from exploding into a crisis.

Once incidents are successfully contained and the recovery process is underway, digital forensic teams should be deployed to identify where the digital evidence resides and acquire it for investigation purposes. This is important to identify the root cause of the incidents. Thus, these processes need to be carried out carefully to ensure that the evidence is accordingly preserved. One of the documents that assist to ensure that the right procedure is conducted is an international standard that provides guidance on identification, collection, acquisition and preservation of digital evidence (International Organization for Standardization, 2012). Since the Internet is borderless, where incidents can cause disputes at cross-border jurisdictions, this international standard is absolutely necessary to ensure that digital evidence acquired can be accepted in the court of laws worldwide. Upon recovery from the incidents, it is important to analyse the causes of the incidents and learn from it to incorporate necessary improvements as part of the process in measuring the effectiveness of security controls deployed.

Security events need to be consistently monitored where security logs from the events in the computer systems should be regularly checked and reviewed by technical management teams. Similarly, as part of security proactive measures, security vulnerabilities should be consistently and periodically assessed to ensure that all systems are updated (patched) and the security measures are in place to avoid vulnerabilities from being exploited.

Due to fast technological changes, organisations should drive security along with consistent security awareness programmes and communicate them effectively. This is inline with the findings in analytical chapter one (sub-section 4.4.8) where security awareness programmes embedded with effective communication can modify the behavioural intention towards compliance. It is also important for the security team to perform continuous monitoring and continual improvement that can be achieved through ISMS implementation.

7.6 Limitations of Study

This study is not bereft of limitations. While the results offer a way out of the negative consequences of the free rider problem, the use of cross sectional data prevents the establishment of causality. While the results are persuasive, they should be treated with caution before generalisations can be made. In addition, future research should focus on cooperative behaviour between organizations and across borders owing to increasing borderless activities that characterize economic activities. Future studies could also attempt to examine causality using longitudinal data. It is also assumed that theories and terminologies have been clearly stated and quoted to provide clarity.

7.7 Suggestion for Future Research

There are several proposals for future research based on the outcome of this study. Future research can focus on aspects where the solution for these areas can be adopted in other countries as cyber security is also a global issue.

This study provided evidence to associate social embeddedness factors with intention to cooperate. This association can be further extended in order to understand the measurement of cooperation that would attain reciprocity as asserted by Axelrod (1984). In addition, the cooperation discussed is within the ecosystem of organisations. Thus, future research should focus on cooperative behaviour between organizations and across borders owing to increasing borderless activities that characterize economic activities.

Furthermore, this study examines only local organisations. For future studies should be be conducted on multinational corporations in order to understand how power distance relate to governance, that can influence decision-making in information security of multi-national corporations. Thus, further gaps can be filled to achieve global cyber security compliance, which can eventually contribute to lowering security breaches. Subsequently, future studies could also attempt to examine causality using longitudinal data. By having this data, the security issue can be understood better through changes of technology trends, institutional change, national and international efforts. Finally, in relating to people problem, future studies can also focus on insider's threat such as disgruntled employees using one of Hofstede's domains; individualist-collectivist domain.

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

Adar, E., & Huberman, B. A. (2000). *Free riding on gnutella*. First Monday, *5*(10-2). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/792/701&lt;/Hu96

Agrawal, A. (2002). Common resources and institutional sustainability. *The drama of the commons*. (pp. 41-85).

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams–Challenges in supporting the organisational security function. *Computers & Security, 31*(5), 643-652.

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management, 35*(6), 717-723.

Ahmed, M., Sharif, L., Kabir, M., & Al-Maimani, M. (2012). Human Errors in Information Security. *International Journal of Advanced Trends in Computer Science and Engineering, 1*(3), 82-87.

Ai Lei Tao. (2015, September). Malaysia the most cyber-savvy nation in Asia claims Eset, but security gaps remain. *ComputerWeekly*. Retrieved from http://www.computerweekly.com/news/4500253424/Malaysia-the-most-cyber-savvy-nation-in-Asia-claims-Eset-but-security-gaps-remain.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. *Action control*. (pp. 11-39): Springer.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Albanese, R., & Van Fleet, D. D. (1985). Rational Behavior in Groups: The Free-Riding Tendency. *Academy of Management. The Academy of Management Review, 10*(2), 244-244.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432-445.

Alchian, A. A., & Demsetz, H. (1972). Production, information costs, and economic organization. *The American Economic Review*, 777-795.

Allan, K. (2014). *Achieving resilience in the cyber ecosystem.* Retrieved from http://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf

Allen, H. B. (1971). Principles of informant selection. *American Speech, 46*(1/2), 47-51.

Anderson, J. C., & Gerbing, D. W. (1988). to_delete_Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin, 103*(3), 411-423.

Anderson, R. (2001). *Why information security is hard - an economic perspective. Proceedings of 17th Annual Computer Security Applications Conference (ACSAC)* New Orleans, La.

Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science, 314*(5799), 610-613.

Andrew, K., & Nada, K.-K. (2000). Future role of IS/IT professionals. *The Journal of Management Development, 19*(2), 97-154.

Antier, C., Kumar, S., Bhagwat, S., & Sankar, R. (2014). Production of fortified food for a public supplementary nutrition program: performance and viability of a decentralised production model for the Integrated Child Development Services Program, India. *Asia Pacific journal of clinical nutrition, 23*(S1), s20-s28.

Apesteguia, J., & Maier-Rigaud, F. P. (2006). The Role of Rivalry Public Goods Versus Common-Pool Resources. *Journal of Conflict Resolution, 50*(5), 646-663.

Araral, E. (2009). What explains collective action in the commons? Theory and evidence from the Philippines. *World Development, 37*(3), 687-697.

Arduin, P.-E., & Vieru, D. (2017). Workarounds as means to identify insider threats to information systems security. *Proceedings of the Twenty-third Americas Conference on Information Systems*.

ARMA International. (2012, October 10). Hackers Breach 52 Universities and Dump Thousands of Personal Records Online. Retrieved from http://www.arma.org/r1/news/washington-policy-brief/2012/10/11/hackers-breach-52-universities-and-dump-thousands-of-personal-records-online

ARMA International. (2016, January 13). Congress Enacts Cyber-Threat Information-Sharing Law. . *ARMA International*. Retrieved from http://www.arma.org/r1/news/washington-policy-brief/2016/01/13/congress-enacts-cyber-threat-information-sharing-law

Armerding, T. (2018, January 26, 2018). *The 17 biggest data breaches of the 21st century*. Retrieved from https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Aronis, S., & Stratopoulos, G. (2016). Implementing business continuity management systems and sharing best practices at a European bank. *Journal of Business Continuity & Emergency Planning, 9*(3), 203-217.

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report, 13*(4), 195-201.

Axelrod, R. (1984). *The evolution of cooperation*. New York, USA: Basic Books, Inc.

Azizan Ramli, Mazlin Mokhtar, & Badhrulhisham Abdul Aziz. (2014). The development of an initial framework for multi-firm industrial safety management based on cooperative relationship: A Malaysia case study. *International Journal of Disaster Risk Reduction, 10, Part A*, 349-361.

Bard, S. K., & Barry, P. J. (2000). Developing a scale for assessing risk attitudes of agricultural decision makers. *The International Food and Agribusiness Management Review, 3*(1), 9-25.

Bardhan, P. (1993). Analytics of the institutions of informal cooperation in rural development. *World Development, 21*(4), 633-639.

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.

Baruch, Y. (1999). Response rate in academic studies-A comparative analysis. *Human Relations, 52*(4), 421-438.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management, 51*(1), 138-151.

Basu, E. (2014, June). Target CEO Fired - Can You Be Fired If Your Company Is Hacked? *Forbes*. Retrieved from http://www.forbes.com.

Batra, D. (2010). The Application of Cognitive Complexity Principles for Reconciling the Agile and the Discipline Approaches. *Advances of Management Information Systems, 18*(1), 13-30.

Baumol, W. J., & Oates, W. E. (1988). *The theory of environmental policy*: Cambridge university press.

BBC. (2011, June 16). Hackers attack Malaysia government websites. *BBC*. Retrieved from http://www.bbc.co.uk/news/world-asia-pacific-13788817

Beautement, A., Sasse, M. A., & Wonham, M. (2009, 7-8 July 2011). *The compliance budget: managing security behaviour in organisations* Proceedings of the 2008 workshop on New security paradigms.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51-61.

Bender, R., & Grouven, U. (1997). Ordinal logistic regression in medical research. *Journal of the Royal College of Physicians of London, 31*(5), 546-551.

Berger, C. R., & Calabrese, R. J. (1975). Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human communication research, 1*(2), 99-112.

Bergkvist, L., & Rossiter, J. R. (2007). The predictive validity of multiple-item versus single-item measures of the same constructs. *Journal of Marketing Research, 44*(2), 175-184.

Bergkvist, L., & Rossiter, J. R. (2009). Tailor-made single-item measures of doubly concrete constructs. *International Journal of Advertising, 28*(4), 607-621.

Bernama. (2010, August 6). Info security plan for critical agencies. *The Star*. Retrieved from https://www.thestar.com.my/news/nation/2010/08/06/info-security-plan-for-critical-agencies/

Bernama. (2011, December 16,). Malaysia ready to face cyber attacks from foreign hackers. *Mysinchew,*. Retrieved from http://www.mysinchew.com/

Bernama. (2015, September 7). Frauds, intrusions, cyber harassment tops list of cyber security incidents in Malaysia *The Malay Mail*. Retrieved from http://www.themalaymailonline.com/

Bernard, H. R. (2011). *Research methods in anthropology: Qualitative and quantitative approaches*: Rowman Altamira.

Berr, J. (2017, May 16). "WannaCry" ransomware attack losses could reach $4 billion. *CBS News*. Retrieved from http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security, 23*(3), 253-264.

Bhunia, P. (2017, October 27). EXCLUSIVE - Safeguarding Malaysian cyber space (Part I) - Protecting critical infrastructure and inculcating public awareness. *Opengov*. Retrieved from http://www.opengovasia.com/articles/7537-exclusive---safeguarding-malaysian-cyber-space-part-i---protecting-critical-national-information-infrastructure-and-inculcating-awareness-amongst-internet-users

Birken, S. A., Lee, S., & Weiner, B. J. (2012). Uncovering middle managers’ role in healthcare innovation implementation. *Implement Science, 7*(1), 28.

Böhme, R. (2006). A comparison of market approaches to software vulnerability disclosure. *Proceedings of Emerging Trends in Information and Communication Security, International Conference, ETRICS 2006*. (pp. 298-311). Freiburg, Germany.

Boman, K. (2012). *Middle East Attacks Highlight Cybersecurity Threat for O&G Industry*. Retrieved from http://www.rigzone.com/news/oil_gas/a/121596/Middle_East_Attacks_Highlight_Cybersecurity_Threat_for_OG_Industry

Bonderud, D. (2016, February 29). *UK Cybercrime on the Rise as Security Confidence Lags*. Retrieved from https://securityintelligence.com/news/uk-cybercrime-on-the-rise-as-security-confidence-lags/

Boulton, C. (2014, September 30). Target's Lack of CISO Was 'Root Cause' of Systems Breach *The Wall Street Journal*. Retrieved from https://www.wsj.com/

Breen, R., Karlson, K. B., & Holm, A. (2013). Total, direct, and indirect effects in logit and probit models. *Sociological Methods & Research, 42*, 164-191.

Bresz, F. (2004). People–Often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance, 6*(4), 57-60.

Brotby, W. K. (2001). *Information Security Governance: Guidance for Boards of Directors and Executive Management 2nd. Edition*. Retrieved from http://www.isaca.org/

Brubaker, E. R. (1975). Free Ride, Free Revelation, or Golden Rule? *Journal of Law and Economics, 18*(1), 147-161.

Brusco, S. (1982). The Emilian model: productive decentralisation and social integration. *Cambridge Journal of Economics, 6*(2), 167-184.

Buchanan, J. M. (1965). Ethical rules, expected values, and large numbers. *Ethics*, 1-13.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of experimental criminology, 11*(1), 97-115.

Burdett, J. (2003). Making groups work: University students' perceptions. *International Education Journal, 4*(3), 177-191.

Burgess, C., & Power, R. (2008). *Secrets stolen, fortunes lost: Preventing intellectual property theft and economic espionage in the 21st century*: Syngress Publishing

Burns, R., & Burns, R. (2008). Logistic Regression. In Business Research Methods and Statistics using SPSS (pp. 568-588): Sage Publication. Retrieved from https://studysites.uk.sagepub.com/burns/website%20material/Chapter%2024%20-%20Logistic%20regression.pdf.

Bursa Malaysia. (2008). *Bursa Malaysia Annual Report 2008*. Retrieved from: http://bursa.listedcompany.com/misc/ar2008/html/corp18/corp18_04.html

Business Cloud News. (2016, February 29). Most data in the cloud is exposed says Thales/Ponemon study. *Business Cloud News*. Retrieved from http://www.businesscloudnews.com/2016/02/29/most-data-in-the-cloud-is-exposed-says-thalesponemon-study/

Camp, L. J., & Wolfram, C. (2000, April 30). *Pricing security.* Proceedings of the Information Survivability Workshop.

Canadian Council of Ministers of the Environment. (2013). *Analysis Of The Free-Rider Issue In Extended Producer Responsibility Programs*. Canada. Retrieved from http://www.publications.gc.ca/site/eng/322866/publication.html.

Carlin, J. (2017, May 17). The 'WannaCry' ransomware attack could have been prevented. Here's what businesses need to know. *CNBC*. Retrieved from http://www.cnbc.com/

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management, 52*(4), 385-400.

Centre for Independent Journalism. (2012, August 14). *Internet Blackout Day on 14 August gaining momentum*. Retrieved from http://cijmalaysia.org/2012/08/14/internet-blackout-day-on-14-august-gaining-momentum/

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of information privacy and security, 1*(3), 18-41.

Chan Wai Kuen, Suhaiza Zailani, & Yudi Fernando. (2009). Critical factors influencing the project success amongst manufacturing companies in Malaysia. *African Journal of Business Management, 3*(1), 16-27.

Chan, Y. H. (2005). Biostatistics 305. Multinomial logistic regression. *Singapore medical journal, 46*(6), 259.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39, Part B*(0), 447-459.

Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security, 16*(5), 484-501.

Churchill, G. A. (1979). A Paradigm for Developing Better Measures of Marketing Constructs. *Journal of Marketing Research, 16*(1), 64-73.

Condon, R. (2010, August). Zurich Insurance breach payment: Data breach fine highest on record. *ComputerWeekly*. Retrieved from http://www.computerweekly.com/news/1519296/Zurich-Insurance-breach-payment-Data-breach-fine-highest-on-record.

Cooper, D. (2006). *The impact of management's commitment on employee behavior: A field study.* Proceedings of the 7th Professional Development Conference & Exhibition, Kingdom of Bahrain.

CSI. (2010). *CSI computer crime and security survey 2010/2011*. Retrieved from http://gocsi.com/survey

Cummings, T. G. (1978). Self-regulating work groups: A socio-technical synthesis. *Academy of management Review, 3*(3), 625-634.

Curtis, J. (2017, June 4). Malware 'stolen from the NSA' cripples the NHS: Hospitals are held to ransom, operations cancelled and A&E patients turned away in global cyber attack using weapon released by 'Shadow Brokers'. *Mail Online*. Retrieved from http://www.dailymail.co.uk/news/article-4501220/Cyber-hackers-cripple-NHS.html

CyberSecurity Malaysia. (2011). *CSM27001 Scheme Policy*. Retrieved from https://csm27001.cybersecurity.my/doc/ISCB-5-POL-2-CSM27001_SP-v1.pdf

CyberSecurity Malaysia. (2013). *ISMS Implementation Guideline-A practical approach*. Retrieved from http://www.cybersecurity.my/data/content_files/11/1170.pdf?.diff=1375349394

CyberSecurity Malaysia. (2018). *MyCERT Incident Statistics*. Retrieved from https://www.mycert.org.my/

D'Onza, G., Lamboglia, R., & Verona, R. (2015). Do IT audits satisfy senior manager expectations? A qualitative study based on Italian banks. *Managerial Auditing Journal, 30*(4/5), 413-434.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207.

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. *Information Systems Management, 22*(1), 77-85.

De Cremer, D., & Van Knippenberg, D. (2002). How do leaders promote cooperation? The effects of charisma and procedural fairness. *Journal of Applied Psychology, 87*(5), 858.

De Jong, J. P., & Den Hartog, D. N. (2007). How leaders influence employees' innovative behaviour. *European Journal of innovation management, 10*(1), 41-64.

Deac, A. (2015). *The Top 10 Worst Cyber Security Breaches from 2013-2015*. Retrieved from https://trushieldinc.com/the-top-10-worst-cyber-security-breaches-from-2013-2015/

Dearden, L. (2015, April 25). Student jailed for hacking University of Birmingham computers to improve his grades. . *The Independent*. Retrieved from http://www.independent.co.uk

Deloitte. (2014). *2014 Deloitte-NASCIO Cybersecurity Study - State governments at risk: Time to move forward*. Retrieved from http://www2.deloitte.com/us/en/pages/public-sector/articles/2014-deloitte-nascio-cybersecurity-study.html

Deneulin, S., & Townsend, N. (2007). Public goods, global public goods and the common good. *International Journal of Social Economics, 34*(1/2), 19-36.

Department of Standards Malaysia. (2017). *Accredited Certification (updated from Q1 2017)*. Retrieved from http://www.jsm.gov.my/schemes-programmes#.Wc3mX8Zx1Vc

Dey, M. (2007, 26-28 September). *Information security management - a practical approach.* AFRICON 2007.

Diamantopoulos, A., Sarstedt, M., Fuchs, C., Wilczynski, P., & Kaiser, S. (2012). Guidelines for choosing between multi-item and single-item scales for construct measurement: a predictive validity perspective. *Journal of the Academy of Marketing Science, 40*(3), 434-449.

Digital News Asia. (2013, November 28). Malaysian Government formulates national cyber-crisis policy. Retrieved from https://www.digitalnewsasia.com/

DiMaggio, P., & Powell, W. W. (1983). The iron cage revisited: Collective rationality and institutional isomorphism in organizational fields. *American Sociological Review, 48*(2), 147-160.

Domański, C. (2010). *Properties of Jarque-Bera test*. Retrieved from http://dspace.uni.lodz.pl/xmlui/handle/11089/340

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies–A case study. *Information Security Technical Report, 14*(4), 223-229.

Evidence (Amendment) (No 2) Act 2012, (2012).

Farrell, H., & Knight, J. (2003). Trust, institutions, and institutional change: Industrial districts and the social capital hypothesis. *Politics & Society, 31*(4), 537-566.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival: Global Politics and Strategy, 53*(1), 23-40.

Finch, B. E., & Spiegel, L. H. (2014). Litigation Following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety Act. *Santa Clara High Technology Law Journal, 30*(3), 349.

Flowerday, S., & Von Solms, R. (2006). Trust: An element of information security. *Security and Privacy in Dynamic Environments*. (pp. 87-98): Springer.

Floyd, S. W., & Wooldridge, B. (1992). Middle management involvement in strategy and its association with strategic type: A research note. *Strategic management journal, 13*(S1), 153-167.

Floyd, S. W., & Wooldridge, B. (1994). Dinosaurs or dynamos? Recognizing middle management's strategic role. *The Academy of Management Executive, 8*(4), 47-57.

Folske-Starlin, H. (2017). *Parental perceptions of effective educators for emotionally impaired students.* (Wayne State University),(Doctor of Philosophy). Available from ProQuest Dissertations & Theses database database. (UMI No.10241836)

Fullerton, A. S., & Xu, J. (2012). The proportional odds with partial proportionality constraints model for ordinal response variables. *Social Science Research, 41*(1), 182-198.

Furnell, S., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers & Security, 75*, 1-9.

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security, 2017*(2), 5-10.

Furnell, S. M., Clarke, N., 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.

Gal-Or, E., & Ghose, A. (2004). The Economic Consequences of Sharing Security Information. *Economics of information security, 12*, 95-104.

Garfinkel, S. L. (2012). The Cybersecurity Risk. *Communications of the ACM, 55*(6), 29-32.

Gartner. (2013). *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020.* Retrieved from http://www.gartner.com/newsroom/id/2636073

Ghannam, J. (2011). *Social Media in the Arab World: Leading up to the Uprisings of 2011*. Retrieved from: http://www.cima.ned.org/wp-content/uploads/2015/02/CIMA-Arab_Social_Media-Report-10-25-11.pdf

Gliem, J. A., & Gliem, R. R. (2003). *Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales*. Retrieved from https://scholarworks.iupui.edu/

Goh Thean Eu. (2015, July 9). Malaysia unveils IoT roadmap, expects US$11bil income boost. *Digital News Asia*. Retrieved from https://www.digitalnewsasia.com/digital-economy/malaysia-unveils-iot-roadmap-expects-usd11bil-income-boost

Gonzalez, J. (2005). Towards a cyber security reporting system–a quality improvement process. *Computer Safety, Reliability, and Security*, 368-380.

González, T. F., & Guillen, M. (2002). Leadership ethical dimension: a requirement in TQM implementation. *the TQM Magazine, 14*(3), 150-164.

Goo, J., Yim, M.-S., & Kim, D. J. (2014). A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate. *Professional Communication, IEEE Transactions on, 57*(4), 286-308.

Gordon, J. N. (2002). Governance failures of the Enron board and the new information order of Sarbanes-Oxley. *Conn. L. Rev., 35*, 1125.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2002). *An economics perspective on the sharing of information related to security breaches: Concepts and empirical evidence*. Proceedings of the First Workshop on Economics and Information Security (May 16-17), University of California, Berkeley. Retrieved from http://www.cpppe.umd.edu/Bookstore/Documents/Economic%20Incentives_05.17.02.pdf

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy, 22*(6), 461-485.

Greco, G., & Floridi, L. (2004). The tragedy of the digital commons. *Ethics and Information Technology, 6*(2), 73-81.

Griffin, M. A., & Neal, A. (2000). Perceptions of safety at work: a framework for linking safety climate to safety performance, knowledge, and motivation. *Journal of occupational health psychology, 5*(3), 347.

Gupta, B., Joshi, R. C., & Misra, M. (2010). Estimating strength of DDoS attack using various regression models. *International Journal of Multimedia Intelligence and Security, 1*(4), 378-391.

Guzzo, R. A., & Shea, G. P. (1992). Group performance and intergroup relations in organizations. *Handbook of industrial and organizational psychology, 3*, 269-313.

Hair, J., Black, W., Babin, B., & Anderson, R. (2010). Multivariate Data Analysis Seventh Edition Prentice Hall.

Hamilton, W. D. (1964). The genetical evolution of social behaviour. II. *Journal of theoretical biology, 7*(1), 17-52.

Hardin, G. (1968). The Tragedy of the Commons. *Science, 162*(3859), 1243-1248.

Hausken, K. (2006). Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy, 25*(6), 629-665.

Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy, 26*(6), 639-688.

Hawkey, K., Muldner, K., & Beznosov, K. (2008). Searching for the right fit: balancing IT security management model trade-offs. *Internet Computing, IEEE, 12*(3), 22-30.

He, Y., Johnson, C., & Lu, Y. (2015). Improving the exchange of lessons learned in security incident reports: case studies in the privacy of electronic patient records. *Journal of Trust Management, 2*(4), 1-20.

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security, 21*(4), 266-287.

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.

Hofstede, G. (1980). Motivation, Leadership, and Organization: Do American Theories Apply Abroad? *Organizational Dynamics, 9*(1), 42-63.

Hofstede, G. (1983). The cultural relativity of organizational practices and theories. *Journal of international business studies*, 75-89.

Holowachuk, B. (2007). Developing an organisation-wide business continuity programme in the public sector: Case study of the Government of Manitoba. *Journal of Business Continuity & Emergency Planning, 2*, 21-32.

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.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security–a neo-institutional perspective. *The Journal of Strategic Information Systems, 16*(2), 153-172.

Huberman, B. A., & Lukose, R. M. (1997). Social dilemmas and Internet congestion. *Science, 277*(5325), 535-537.

Hurwitz, R., Lin, H., Libicki, M. C., & Yannakogeorgos, P. A. (2012). Depleted Trust in the Cyber Commons. *STRATEGIC STUDIES, 21*(3), 20-45.

Hwang, A., & Francesco, A. M. (2010). The influence of individualism–collectivism and power distance on use of feedback channels and consequences for learning. *Academy of Management Learning & Education, 9*(2), 243-257.

Hylton, K. N. (2007). Property Rules, Liability Rules, and Immunity: An Application to Cyberspace. *BUL Rev., 87*, 1.

Ida Madieha Abdul Ghani, Sonny Zulhuda, & Sigit Puspito Wigati Jarot. (2012). Data leak, critical information infrastructure and the legal options: what does Wikileaks teach us? *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1*(3), 226-231.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79.

Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security, 25*(7), 498-506.

Iizuka, M., & Katz, J. M. (2010). *Natural resource industries,'tragedy of the commons' and the case of Chilean salmon farming*: UNU-MERIT, Maastricht Economic and Social Research and Training Centre on Innovation and Technology.

International Organization for Standardization. (2011). *ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management*

International Organization for Standardization. (2012). *ISO/IEC 27014: 2012 Information technology — Security techniques —Governance of information security*

International Organization for Standardization. (2012). *ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity*

International Organization for Standardization. (2012). *ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines on Identification, Collection, Acquisition and Preservation of Digital Evidence*

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information Technology - Security techniques-Information security management systems-Requirements*

International Organization for Standardization. (2013). *ISO/IEC 27002: 2013 Information technology — Security techniques — Code of practice for information security controls*

International Organization for Standardization. (2014). *ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary*

International Telecommunications Union. (2017). *Global Cybersecurity Index 2017*. Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Internet World Stats. (2017). *ASIA INTERNET USE, POPULATION DATA AND FACEBOOK STATISTICS - JUNE 2017*. Retrieved from http://www.internetworldstats.com/stats3.htm#asia

Isaac, R. M., & Walker, J. M. (1988). Communication and free-riding behavior: The voluntary contribution mechanism. *Economic Inquiry, 26*(4), 585-608.

ISACA. (2011). *Cism Review Manual 2012*. USA: ISACA.

ISACA. (2012). *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT*. Retrieved from http://www.isaca.org/cobit/Pages/CobitFramework.aspx

ISO/IEC27001. (n.d.). Retrieved from http://www.iso27001security.com/html/27001.html

Israel, G. D. (1992). *Determining sample size*. Retrieved from http://edis.ifas.ufl.edu/pd006,

Itoh, H. (1992). Cooperation in hierarchical organizations: An incentive perspective. *Journal of Law, Economics, & Organization*, *8*(2), 321-345.

Jacqueline, H. H., Shahram, S., & Thomas, A. M. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, *19*(3), 155-176.

Janis, I. L. (1967). Effects of fear arousal on attitude change: Recent developments in theory and experimental research. *Advances in experimental social psychology, 3*, 166-224.

Jarque, C. M., & Bera, A. K. (1987). A test for normality of observations and regression residuals. *International Statistical Review/Revue Internationale de Statistique*, 163-172.

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, *33*(3), 583-590.

Jeffries, F. L., & Becker, T. E. (2008). Trust, norms, and cooperation: Development and test of a simplified model. *Journal of Behavioral and Applied Management, 9*(3), 316.

Jerdee, T. H., & Rosen, B. (1974). Effects of opportunity to communicate and visibility of individual decisions on behavior in the common interest. *Journal of Applied Psychology, 59*(6), 712-716.

Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*(5), 413-422.

Johansen, L. (1977). The theory of public goods: Misplaced emphasis? *Journal of Public Economics, 7*(1), 147-152.

Johnson, C. W. (2014). Inadequate legal, regulatory and technical guidance for the forensic analysis of cyber-attacks on safety-critical software. *Proceedings of the 32nd International Systems Safety Society, Louisville, USA. International Systems Safety Society, Unionville*.

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*(3), 16-24.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly, 34*(3), 549-566.

Juhee, K., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector *MIS Quarterly, 38*(2), 451-471.

Kabay, M. (1994). Psychosocial factors in the implementation of information security policy. *EDPACS: The EDP Audit, Control, and Security Newsletter, 21*(10), 1-10.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Karlson, K. B., & Holm, A. (2011). Decomposing primary and secondary effects: a new decomposition method. *Research in Social Stratification and mobility, 29*(2), 221-237.

Kaul, I., Grungberg, I., & Stern, M. A. (1999). *Global Public Goods: International Cooperation in the 21st Century* Oxford, England: Oxford University Press.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly executive, 9*(3), 2012-2052.

Kelman, H. C. (1958). Compliance, identification, and internalization three processes of attitude change. *Journal of Conflict Resolution, 2*(1), 51-60.

Khalifa, M., & Khalid, P. (2015). Developing Strategic Health Care Key Performance Indicators: A Case Study on a Tertiary Care Hospital. *Procedia Computer Science, 63*, 459-466.

Kiggundu, M. N. (1981). Task Interdependence and the Theory of Job Design. *The Academy of Management Review, 6*(3), 499-508.

Killingback, T., & Doebeli, M. (2002). The continuous prisoner’s dilemma and the evolution of cooperation through reciprocal altruism with variable investment. *The American Naturalist, 160*(4), 421-438.

Kim Wai Lam, Aminuddin Hassan, Tajularipin Sulaiman, & Nurzatulshima Kamarudin. (2018). Instructional Technology Competencies as Perceived by University Lecturers in Malaysia. *International Journal of Academic Research in Business and Social Sciences, 8*(3), 401-417.

Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security, 25*(7), 522-538.

Knapp, K. J., Franklin Morris Jr, R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security, 28*(7), 493-508.

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36.

Kocmanova, A., & Simberova, I. (2012). Modelling of corporate governance performance indicators. *Engineering Economics, 23*(5), 485-495.

Kohler, U., Karlson, K. B., & Holm, A. (2011). Comparing coefficients of nested nonlinear probability models. *Stata Journal, 11*(3), 420-438.

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security, 33*(0), 3-11.

Kollock, P. (1998). Social Dilemmas: The Anatomy of Cooperation. *Annual Review of Sociology, 24*, 183-214.

Kostova, T. (1999). Transnational transfer of strategic organizational practices: A contextual perspective. *Academy of management Review, 24*(2), 308-324.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren’t more information security research studies. *Information & Management, 41*(5), 597-607.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security, 28*(7), 509-520.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security, 27*(5), 224-231.

Kritzinger, E., & Von Solms, S. H. (2005). *Five Non-Technical Pillars of Network Information Security Management.* Communications and Multimedia Security.

Kwon, J., & Johnson, M. E. (2011). *The impact of security practices on regulatory compliance and security performance.* Proceedings of the 32nd International Conference on Information Systems, AIS. Shanghai.

Kwon, J., Ulmer, J. R., & Wang, T. (2012). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems, 27*(1), 219-236.

Langevin, J. R., McCaul, M. T., Charney, S., & Raduege, H. (2008). *Securing Cyberspace for the 44th Presidency*. Washington, D.C: Retrieved from: https://www.nitrd.gov/cybersecurity/documents/081208_securingcyberspace_44.pdf

Langham, J. A., Paulsen, N., & Härtel, C. E. (2012). Improving tax compliance strategies: Can the theory of planned behaviour predict business compliance? *eJournal of Tax Research, 10*(2), 364.

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy, 9*(3), 49-51.

Lant, C. L., Ruhl, J. B., & Kraft, S. E. (2008). The Tragedy of Ecosystem Services. *BioScience, 58*(10), 969-974.

Lee, J. W., Song, J. G., Lee, C. K., & Lee, D. Y. (2012). A Conceptual Framework for Securing Digital I&C Systems in Nuclear Power Plants. *Proceedings of the International Conference on Security and Management (SAM).* (pp. 1-7). Athens.

Lemos, R. (2015). *Private market growing for zero-day exploits and vulnerabilities*. Retrieved from http://searchsecurity.techtarget.com/feature/Private-market-growing-for-zero-day-exploits-and-vulnerabilities

Leonard, L. N., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management, 42*(1), 143-158.

Liden, R. C., Sparrowe, R. T., & Wayne, S. J. (1997). Leader-member exchange theory: The past and potential for the future. *Research in personnel and human resources management, 15*, 47-120.

Line, M. B. (2013). *A case study: Preparing for the smart grids-identifying current practice for information security incident management in the power industry.* 2013 Seventh International Conference on IT Security Incident Management and IT Forensics.

Line, M. B., Albrechtsen, E., Jaatun, M. G., Tøndel, I. A., Johnsen, S. O., Longva, O. H., & Wærø, I. (2008). *A structured approach to incident response management in the oil and gas industry.* International Workshop on Critical Information Infrastructures Security.

Little, R. J., & Rubin, D. B. (2002). *Statistical analysis with missing data* (2nd ed.). Hoboken, New Jersey: John Wiley & Sons.

Liu, W., Tanaka, H., & Matsuura, K. (2008). Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms. *Information and Media Technologies, 3*(2), 464-478.

Lukasik, S. J. (2000). Protecting the global information commons. *Telecommunications Policy, 24*(6–7), 519-531.

Lukasik, S. J. (2011). Protecting users of the cyber commons. *Commun. ACM, 54*(9), 54-61.

MacKinnon, D. P., Fairchild, A. J., & Fritz, M. S. (2007). Mediation analysis. *Annual Review of Psychology, 58*(1), 593-614.

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and social psychology Bulletin, 18*(1), 3-9.

Marquaridt, D. W. (1970). Generalized inverses, ridge regression, biased linear estimation, and nonlinear estimation. *Technometrics, 12*(3), 591-612.

Marwell, G., & Ames, R. E. (1981). Economists free ride, does anyone else?: Experiments on the provision of public goods, IV. *Journal of Public Economics, 15*(3), 295-310.

Maslina Daud, 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.

McConnell, M., Chertoff, M., & Lynn, W. (2012). *China's Cyber Thievery Is National Policy -- And Must Be Challenged.* Wall Street Journal, A.15. Retrieved from http://search.proquest.com/docview/918023651?accountid=28930

McElligott, T. (2006). Penetration Testing Digs Deeper *Telephony, 247*(16), 40-43.

McGourty, J. (1998). *Strategies for developing, implementing, and institutionalizing a comprehensive assessment process for engineering education.* Frontiers in Education Conference, 1998. Tempe, AZ, USA.

McNeil, K., & Thompson, J. D. (1971). The regeneration of social organizations. *American Sociological Review*, 624-637.

Melis, A. P., & Semmann, D. (2010). How is human cooperation different? *Philosophical Transactions of the Royal Society B: Biological Sciences, 365*(1553), 2663-2674.

Merritt, A. (2000). Culture in the cockpit do Hofstede's dimensions replicate? *Journal of cross-cultural psychology, 31*(3), 283-301.

Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology, 83*(2), 340-363.

Miller, M. E. (2015, September 24). 'Car hacking' just got real: In experiment, hackers disable SUV on busy highway. *The Register*. Retrieved from http://www.theregister.co.uk/2015/09/24/arin_ipv4_interview_ipv6

Ministry of Science Technology and Innovation. (2012). *Guideline to Determine Information Security Professionals Requirements for the CNII Agencies / Organisations*. Retrieved from http://www.cybersecurity.my/data/content_files/11/1159.pdf?.diff=1373447691.

Ministry of Science Technology and Innovation. (July 2006). *National Cyber Security Policy: The Way Forward*. Kuala Lumpur, Malaysia.

Mohamed, D. b. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review, 29*(1), 66-76.

Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity Challenges and Compliance Issues within the US Healthcare Sector. *International Journal of Business and Social Research, 5*(02), 55-66.

Moore, S. (2014, August 22, 2014). Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware. Retrieved from http://www.gartner.com/newsroom/id/2828722

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 3*(3–4), 103-117.

Moss, S., Prosser, H., Costello, H., Simpson, N., Patel, P., Rowe, S., . . . Hatton, C. (1998). Reliability and validity of the PAS - ADD Checklist for detecting psychiatric disorders in adults with intellectual disability. *Journal of Intellectual Disability Research, 42*(2), 173-183.

Mulder, L. B., van Dijk, E., & De Cremer, D. (2009). When sanctions that can be evaded still work: The role of trust in leaders. *Social Influence, 4*(2), 122-137.

Mulej, M., Rebernik, M., & Bradac, B. (2006). Cooperation and opportunistic behaviour in transformational outsourcing. *Kybernetes, 35*(7/8), 1005-1013.

Muniandy, L., & Muniandy, B. (2012). State of cyber security and the factors governing its protection in Malaysia. *International Journal of Applied Science and Technology, 2*(4).

Murphy, K., Tyler, T. R., & Curtis, A. (2009). Nurturing regulatory compliance: Is procedural justice effective when people question the legitimacy of the law? *Regulation & governance, 3*(1), 1-26.

Musa, N. (2012). *Role of the boards and senior management within formal, technical and informal components: IS/IT security governance in the Malaysian publicly listed companies.* University of Tasmania.

National Audit Office. (2013). *The UK cyber security strategy: Landscape review*. Retrieved from http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Security Council. (2012). *Directive No. 24 National Cyber Crisis Management Mechanism and Policy.* . Kuala Lumpur, Malaysia.

Nelson, R. R., & Winter, S. G. (1982). An evolutionary theory of economic change. *Harvard Business School Press, Cambridge*.

Nelson, R. R., & Winter, S. G. (2002). Evolutionary Theorizing in Economics. *The Journal of Economic Perspectives*, *16*(2), 23-46.

Newman, J. (2011, May). Experts on PSN Hack: Sony Could Have Done More. *PcWorld*. Retrieved from http://www.pcworld.com/article/227770/experts_on_psn_hack_sony_could_ve_done_more.html.

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security, 31*(4), 418-436.

Noor Ismawati Jaafar, & Adnan Ajis. (2013). Organizational climate and individual factors effects on information security compliance behaviour. *International Journal of Business and Social Science, 4*(10).

North, D. C. (1991). Institution. *Journal of Economic Perspectives, 5*(1), 97-112.

North, D. C. (1994). Economic performance through time. *The American Economic Review, 84*(3), 359-359.

Norton. (2012). *2012 NORTON CYBERCRIME REPORT*. Retrieved from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Nunnally, J. C. (1978). *Psychometric theory*: McGraw-Hill New York.

Ohlheiser, A. (2013, July 10). Malcolm Gladwell's Cockpit Culture Theory and the Asiana Crash. *The Wire*. Retrieved from http://www.thewire.com/national/2013/07/malcolm-gladwells-cockpit-culture-theory-everywhere-after-asiana-crash/67058/

Olson, M. (1965). The logic of collective action: Public goods and the theory of groups. In. Cambridge, MA: Harvard University Press.

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Retrieved from http://wtf.tw/ref/ostrom_1990.pdf

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance.* System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

Pais, J. (2014). Cumulative structural disadvantage and racial health disparities: The Pathways of childhood socioeconomic influence. *Demography, 51*(5), 1729-1753.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*.

Pasa, S. F. (2000). Leadership influence in a high power distance and collectivist culture. *Leadership & Organization Development Journal, 21*(8), 414-426.

Peduzzi, P., Concato, J., Kemper, E., Holford, T. R., & Feinstein, A. R. (1996). A simulation study of the number of events per variable in logistic regression analysis. *Journal of clinical epidemiology, 49*(12), 1373-1379.

Permann, M. R., & Rohde, K. (2005). *Cyber assessment methods for SCADA security. 15th Annu. Joint ISA POWID/EPRI Controls and Instrumentation Conf., Nashville, TN.* Retrieved from http://scadahacker.com/library/Documents/Assessment_Guidance/ISA%20-%20Paper%20-%20Cyber%20Assessments%20Methods%20for%20SCADA.pdf

Peterson, A. (2014, December 8). Why cyber armies are a good investment for countries like North Korea. *The Washington Post*. Retrieved from https://www.washingtonpost.com/

Pfeiffer, T., & Nowak, M. A. (2006). Digital cows grazing on digital grounds. *Current Biology, 16*(22), R946-R949.

Pinsonneault, A., & Kraemer, K. (1993). Survey research methodology in management information systems: an assessment. *Journal of management information systems, 10*(2), 75-105.

Piore, M. S., & Sabel, C. F. C.(1984): The Second Industrial Divide. Possibilities for Prosperity. In: Basic Books, New York.

Ponemon Institute. (2010). *2010 Annual Study: U.S. Cost of a Data Breach*. Retrieved from http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf

Ponemon Institute. (2014). *2014 Cost of Data Breach Study: Global Analysis*. Retrieved from Ponemon Institute website: http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

Ponemon Institute. (2015). *2015 Cost of Data Breach Study Global Analysis*. Retrieved from:http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF

Ponemon Institute. (2016). *2016 Cost of Data Breach Study: Global Analysis*. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

Ponemon Institute. (2017). *2017 Cost of Data Breach Study: Global Overview*. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

Pope, C., & Mays, N. (1995). Reaching the parts other methods cannot reach: an introduction to qualitative methods in health and health services research. *BMJ: British Medical Journal, 311*(6996), 42.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security, 26*(3), 229-237.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.

Poteete, A. R., & Ostrom, E. (2004). Heterogeneity, group size and collective action: The role of institutions in forest management. *Development and change, 35*(3), 435-461.

Powell, B. (2005). Is Cyberspace a Public Good-Evidence from the Financial Services Industry. *Journal of Law Economics & Policy, 1,* 497-510.

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.

PricewaterhouseCoopers. (2012). *Changing the game Key findings from The Global State of Information Security Survey 2013*. Retrieved from http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml

PricewaterhouseCoopers. (2016). *Global Economic Crime Survey 2016*. Retrieved from: http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

Proviti. (2016). *Arriving at Internal Audit's Tipping Point Amid Business Transformation*. Retrieved from http://www.protiviti.com/en-US/Documents/Surveys/2016-Internal-Audit-Capabilities-and-Needs-Survey-Protiviti.pdf

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly, 34*(4), 757-778.

Pye, G., & Warren, M. (2005). *Benchmarking e-business security: A model and framework.* Proceeding of the 3rd Australian Computer, Network & Information Forensics Conference.

Quine, L., Rutter, D. R., & Arnold, L. (1998). Predicting and understanding safety helmet use among schoolboy cyclists: a comparison of the theory of planned behaviour and the health belief model. *Psychology and Health, 13*(2), 251-269.

Radianti, J., Rich, E., & Gonzalez, J. J. (2009, 5-8 Jan. 2009). *Vulnerability Black Markets: Empirical Evidence and Scenario Simulation.* System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference

Ramamoorthy, N., & Flood, P. C. (2004). Individualism/collectivism, perceived task interdependence and teamwork attitudes among Irish blue-collar employees: a test of the main and moderating effects? *Human Relations, 57*(3), 347-366.

Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How Effective Is Your Security Awareness Program? An Evaluation Methodology. *Information Security Journal: A Global Perspective, 21*(6), 328-345.

Rasiah, R. (1994). Flexible production systems and local machine-tool subcontracting: electronics components transnationals in Malaysia. *Cambridge Journal of Economics, 18*(3), 279-298.

Rasiah, R. (2011). The Role of Institutions and Linkages in Learning and Innovation. *Institutions and Economies, 3*(2), 165-172.

Razana, M., & Shafiuddin, Z. (2016). CyberSecurity Malaysia: Towards Becoming a National Certification Body for Information Security Management Systems Internal Auditors. *World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, 10*(8), 2881-2884.

Ree, M., & Robertson, J. (2015, November 2015). It's Way Too Easy to Hack the Hospital. *Bloomberg Businessweek*. Retrieved from http://www.bloomberg.com/features/2015-hospital-hack/

Reich, B. H., & Benbasat, I. (2000). Factors that influence the social dimension of alignment between business and information technology objectives. *MIS Quarterly*, 81-113.

Reingold, J. (2008, November 19). Secrets of their success. *Fortune Magazine*. Retrieved from http://archive.fortune.com/2008/11/11/news/companies/secretsofsuccess_gladwell.fortune/index.htm.

Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security, 20*(4), 296-311.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014). *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*. Bloomberg Business. Retrieved from http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data

Risvold, M. O. (2010). Organizational issues related to information security behavior. *Lulea University of Technology*, 1653-0187.

Robertson, J., & Riley, M. (2014, August 24). JPMorgan, Four Other Banks Hit by Hackers: U.S. Official. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/articles/2014-08-27/customer-data-said-at-risk-for-jpmorgan-and-4-more-banks

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*, 90-110.

Rodríguez, N. G., Pérez, M. J. S., & Gutiérrez, J. A. T. (2008). Can a good organizational climate compensate for a lack of top management commitment to new product development? *Journal of Business Research, 61*(2), 118-131.

Rosenzweig, P. (2012). *Cybersecurity and Public Goods-The Public/Private "Partnership"*. Cyberwarfare: How Conflicts in Cyberspace are Challenging America and Changing the World. Retrieved from http://media.hoover.org/

Rosenzweig, P. (2012). Cybersecurity and Public Goods-The Public/Private "Partnership". In Cyberwarfare: How Conflicts in Cyberspace are Challenging America and Changing the World Praeger. Retrieved from http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf.

Rossiter, J. R. (2002). The C-OAR-SE procedure for scale development in marketing. *International journal of research in marketing, 19*(4), 305-335.

Rozek, P., & Groth, D. (2008). Business Continuity Planning. *Health management technology, 29*(3), 10.

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.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-66.

Sally, D. (1995). Conversation and cooperation in social dilemmas a meta-analysis of experiments from 1958 to 1992. *Rationality and society, 7*(1), 58-92.

Samuelson, P. A. (1954). The pure theory of public expenditure. *The review of economics and statistics, 36*(4), 387-389.

Sanders, K., Schyns, B., Sanders, K., & Schyns, B. (2006). Trust, conflict and cooperative behaviour: Considering reciprocity within organizations. *Personnel Review*, *35*(5), 508-518.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal, 19*(3), 122-131.

Schalk, R., & Curşeu, P. L. (2010). Cooperation in organizations. *Journal of Managerial Psychology, 25*(5), 453-459.

Schneider, F., & Pommerehne, W. W. (1981). Free Riding and Collective Action: An Experiment in Public Microeconomics. *The Quarterly Journal of Economics, 96*(4), 689-704.

Schneier, B. (2000). *Secrets and lies: digital security in a networked world*. New York: John Wiley & Sons, Inc.

Schneier, B. (2007). *Information Security and Externalities*. ENISA Quarterly, *2*(4), 3-4. Retrieved from http://www.oecd.org/sti/interneteconomy/37985707.pdf

Scott, D., Bishop, J. W., & Chen, X. (2003). An examination of the relationship of employee involvement with job satisfaction, employee cooperation, and intention to quit in US invested enterprise in China. *The International Journal of Organizational Analysis, 11*(1), 3-19.

Seals, T. (2015, September 30). Target Breach Costs Could Total $1Bn. *Infosecurity Magazine, September*. Retrieved from http://www.infosecurity-magazine.com/news/target-breach-costs-could-total-1bn/.

Sengenberger, W., Loveman, G., & Piore, M. J. (1990). *The re-emergence of small enterprises: industrial restructuring in industrialised countries*: International Labour Organisation.

Setbon, M., & Raude, J. (2010). Factors in vaccination intention against the pandemic influenza A/H1N1. *The European Journal of Public Health, 20*(5), 490-494.

Shamir b. Hashim, M. (2011). *Malaysia's National Cyber Security Policy: The country's cyber defence initiatives*. Cybersecurity Summit (WCS), 2011 Second Worldwide, 1-7. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5978782

Shamir b. Hashim, M. (2017). *National Cybersecurity Governance and Implementation of Malaysia for the Critical National Information Infrastructure*. Asia Research Policy, *8*(1), 79-87. Retrieved from http://www.arpjournal.org/usr/browse/view_issues_detail.do?seq=147

Sharp, S., & Smith, P. K. (1991). Bullying in UK schools: The DES Sheffield bullying project. *Early Child Development and Care, 77*(1), 47-55.

Shavell, S. (1980). Strict Liability versus Negligence. *The Journal of Legal Studies, 9*(1), 1-25.

Shedden, P., Ahmad, A., & Ruighaver, A. (2010). Organisational learning and incident response: promoting effective learning through the incident response process.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees’ adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Smith, K. G., Carroll, S. J., & Ashford, S. J. (1995). Intra-and interorganizational cooperation: Toward a research agenda. *Academy of Management journal, 38*(1), 7-23.

Smith, K. G., Smith, K. A., Olian, J. D., Sims, H. P., O'Bannon, D. P., & Scully, J. A. (1994). Top Management Team Demography and Process: The Role of Social Integration and Communication. *Administrative Science Quarterly, 39*(3), 412-438.

Sobel, M. E. (1982). Asymptotic confidence intervals for indirect effects in structural equation models. *Sociological methodology, 13*(1982), 290-312.

Solum, L. (2010). *Questioning Cultural Commons*. Cornell Law Review, *95*, 09-24. Retrieved from HeinOnLine database

Son, H., & Riley, M. (2014, October 3). JPMorgan Password Leads Hackers to 76 Million Households. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/articles/2014-10-03/jpmorgan-password-said-to-lead-hackers-to-76-million-households

Sonny Zulhuda. (2011). National security in Malaysia's digital economy: redefinition, reaction and legal reform. *Journal of Applied Sciences Research, 7*(13), 2316-2325.

Sonny Zulhuda. (2012). The state of e-government security in Malaysia: reassessing the legal and regulatory framework on the threat of information theft.

Spector, P. E. (1992). Summated Rating Scale Construction: An IntroductionSage. *Newbury Park, CA.*

Starr, B., & Yan, H. (2013, June 23). Man behind NSA leaks says he did it to safeguard privacy, liberty. *CNN*. Retrieved from http://edition.cnn.com/2013/06/10/politics/edward-snowden-profile/

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems, 13*(3), 228-243.

Stevenson, A. (2015). *Chinese hackers hit top US university with data harvesting attacks*. Retrieved from http://www.v3.co.uk/v3-uk/news/2408952/chinese-hackers-hit-top-us-university-with-data-harvesting-attacks

Stigler, G. J. (1974). Free Riders and Collective Action: An Appendix to Theories of Economic Regulation. *The Bell Journal of Economics and Management Science, 5*(2), 359-365.

Stiglitz, J. E. (1985). Information and economic analysis: a perspective. *The Economic Journal, 95*, 21-41.

Stinnett, J. P. (2017). *Over the hurdle: A quantitative study examining the obstacles of achieving professional certification and the perceived effective practices for overcoming them.* Syracuse University.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 441-469.

Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Straub Jr, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly, 14*(1), 45-60.

Streiner, D. L., & Norman, G. R. (1989). *Health measurement scales: a practical guide to their development and use*: Oxford university press.

Strohm, C., & Engleman, E. (2012, September 28). Cyber Attacks on U.S. Banks Expose Computer Vulnerability. *Bllomberg Business*. Retrieved from http://www.bloomberg.com/

Suhazimah Dzazali, Ainin Sulaiman, & Ali Hussein Zolait. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly, 26*(4), 584-593.

Suhazimah Dzazali, & Ali Hussein Zolait. (2012). Assessment of information security maturity: an exploration study of Malaysian public service organizations. *Journal of Systems and Information Technology, 14*(1), 23-57.

Suhr, D., & Shay, M. (2009). *Guidelines for reliability, confirmatory and exploratory factor analysis.* Proc. 2009 Western Users of SAS Conf. San Jose, CA.

Sull, D. N. (2003). Managing by commitments. *Harvard Business Review, 81*(6), 82-91, 137.

Swarts, P. (2015, February 2). Obama budget dedicates $14B to cybersecurity. *The Washington Times.* Retrieved from http://www.washingtontimes.com

Sweetman, K. (2012). *In Asia, Power Gets in the Way*. Retrieved from https://hbr.org/2012/04/in-asia-power-gets-in-the-way/

Taylor, S., & Todd, P. (1995). Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions. *International journal of research in marketing, 12*(2), 137-155.

Teh, P.-L., Ooi, K.-B., & Yong, C.-C. (2008). Does TQM impact on role stressors? A conceptual model. *Industrial Management & Data Systems, 108*(8), 1029-1044.

Teo, T. S., & Ang, J. S. (1999). Critical success factors in the alignment of IS plans with business plans. *International Journal of Information Management, 19*(2), 173-185.

Thabane, L., Ma, J., Chu, R., Cheng, J., Ismaila, A., Rios, L. P., . . . Goldsmith, C. H. (2010). A tutorial on pilot studies: the what, why and how. *BMC medical research methodology, 10*(1), 1.

Thadewald, T., & Büning, H. (2007). Jarque–Bera test and its competitors for testing normality–a power comparison. *Journal of Applied Statistics, 34*(1), 87-105.

Thales. (2018). *2018 Thales Data Threat Report*. Retrieved from https://www.thalesgroup.com/sites/default/files/asset/document/2018-data-threat_report-global-edition.pdf

The Malaysian Insider. (2011, June 15). Malaysia bracing for Anonymous onslaught, says IGP. *The Malaysian Insider*. Retrieved from http://www.themalaysianinsider.com/malaysia/article/malaysia-bracing-for-anonymous-onslaught-says-igp

The Sun Daily. (2014, February 4). 46,000 medical images wiped out in UMMC. *The Sun Daily*. Retrieved from http://www.thesundaily.my/news/948355

The White House. (2013). *Presidential Policy Directive -- Critical Infrastructure Security and Resilience.* Retrieved from https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

The White House. (2015). *Executive Order -- Promoting Private Sector Cybersecurity Information Sharing*. Retrieved from https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

Thomas, E. J. (1957). Effects of facilitative role interdependence on group functioning. *Human Relations*.

Titcomb, J., & McGoogan, C. (2017, May 15). Cyber attack: Latest evidence indicates 'phishing' emails not to blame for global hack. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42-57.

Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and Applications 5*, 147–158.

Tov, W., & Diener, E. (2008). The well-being of nations: Linking together trust, cooperation, and democracy. *Cooperation: The political psychology of effective human interaction*, 323-342.

Trivers, R. L. (1971). The evolution of reciprocal altruism. *Quarterly review of biology, 46*(1), 35-57.

Tyler, T. R., & Fagan, J. (2008). Legitimacy and cooperation: Why do people help the police fight crime in their communities. *Ohio St. J. Crim. L., 6*, 231.

Tyran, J. R., & Feld, L. P. (2006). Achieving Compliance when Legal Sanctions are Non‐deterrent. *The Scandinavian Journal of Economics, 108*(1), 135-156.

U.S. Food and Drug Administration. (2014). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices-Guidance for Industry and Food and Drug Administration Staff*. October 2, 2014. Retrieved from http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm356190.pdf

U.S. Food and Drug Administration. (2015). *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*. July 31, 2015. Retrieved from http://www.fda.gov/

Vaas, L. (2012). *US senator blames Iran for cyber attacks on banks*. Retrieved from http://nakedsecurity.sophos.com/2012/09/26/us-iran-banks/

Valentine, A. J. (2010). Compliance complacency: How ‘check-box’ compliancy remains a pitfall for many organizations worldwide. *Information Security Technical Report, 15*(4), 154-159.

Van Der Vegt, G., Emans, B., & Van De Vliert, E. (1999). Effects of Interdependencies in Project Teams. *The Journal of Social Psychology*, *139*(2), 202-214.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3), 190-198.

Varian, H. V. (2000, June 1). Managing Online Security Risks. *The New York Times*. Retrieved from http://www.nytimes.com/library/financial/columns/060100econ-scene.html

Veblen, T. (1915). *Imperial Germany and the industrial revolution*. London, England: MacMillan.

Veiga, A. D., & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information Systems Management, 24*(4), 361-372.

Venter, W., Kruger, S., & Herbst, F. (2007). A proposed conceptual familiness transmission of capital model. *South African Journal of Business Management, 38*(3), 1-14.

Verizon. (2013). *2013 Data Breach Investigations Report*. Retrieved from Verizon website: http://www.verizonenterprise.com/DBIR/2013/

Vieira, J. (2005). Water safety plans: methodologies for risk assessment and risk management in drinking-water systems. *IAHS-AISH Publication 310*, 57-67.

Viki, G. T., Culmer, M. J., Eller, A., & Abrams, D. (2006). Race and willingness to cooperate with the police: The roles of quality of contact, attitudes towards the behaviour and subjective norms. *British Journal of Social Psychology, 45*(2), 285-302.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*(5), 371-376.

Von Solms, R. (1997). Driving safely on the information superhighway. *Information Management & Computer Security, 5*(1), 20-22.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*(0), 97-102.

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security, 23*(4), 275-279.

Von Solms, R., & Von Solms, S. H. (2006). Information Security Governance: A model based on the Direct–Control Cycle. *Computers & Security, 25*(6), 408-412.

Von Solms, S. B. (2005). Information Security Governance–compliance management vs operational management. *Computers & Security, 24*(6), 443-447.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Wageman, R. (1995). Interdependence and group effectiveness. *Administrative Science Quarterly*, 145-180.

Wagner, A., & Brooke, C. (2007). Wasting time: The mission impossible with respect to technology-oriented security approaches. *Electronic Journal of Business Research Methods, 5*(2), 117-124.

Wagner, J. A. (1995). Studies of individualism-collectivism: Effects on cooperation in groups. *Academy of Management journal*, *38*(1), 152-173.

Waljee, J. F., Chung, K. C., Kim, H. M., Burns, P. B., Burke, F. D., Wilgis, E. F. S., & Fox, D. A. (2010). Validity and responsiveness of the Michigan hand questionnaire in patients with rheumatoid arthritis: A multicenter, international study. *Arthritis Care & Research, 62*(11), 1569-1577.

Warren, M., & Leitch, S. (2011). *Australian national critical infrastructure protection : a case study.* Proceedings of the 10th European Conference on Information Warfare and Security, Academic Conference Limited. Reading, England.

Wilkinson, F. (2013). *The dynamics of labour market segmentation*. London, UK: Academic Press.

Williams, P. (2001). Information security governance. *Information Security Technical Report, 6*(3), 60-70.

Williams, P. A. (2008). In a ‘trusting’environment, everyone is responsible for information security. *Information Security Technical Report, 13*(4), 207-215.

Williamson, W. (2014, June 18). The Underground Economy of Data Breaches. *Forbes*. Retrieved from http://www.forbes.com/sites/frontline/2014/06/18/the-underground-economy-of-data-breaches/#23d110b26c72

Wood, C. C. (1997). Policies alone do not constitute a sufficient awareness effort. *Computer Fraud & Security, 1997*(12), 14-19.

World Economic Forum. (2015). *Global Risks 2015 10th Edition*. Retrieved from: http://reports.weforum.org/global-risks-2015/

Wylder, J. O. (2003). Improving security from the ground up. *Information Systems Security, 11*(6), 29-38.

Yamane, T. (1967). *STATISTICS; An Introductory Analysis* (2nd. ed.): New York: Harper and Row.

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems, 92*, 36-46.

Zahri Yunos, Nor'azuwa Muhamad Pahri, Mohd Shamir Hashim, & Rahayu Ahmad. (2014). Adoption of ISMS for Protecting SCADA Systems against Cyber Terrorism Threats. *03*(04).

Zahri Yunos, Syahrul Hafidz Suid, Rabiah Ahmad, & Zuraini Ismail. (2010). *Safeguarding Malaysia's critical national information infrastructure (CNII) against cyber terrorism: Towards development of a policy framework.* Information Assurance and Security (IAS), 2010 Sixth International Conference on.

LIST OF PUBLICATIONS

1. Maslina Daud, 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.

2. Maslina Daud, Rasiah, R., George, M., Asirvatham, D., Abdul Fuad Abdul Rahman, & Azni Ab Halim. (2018). Denial of Service (DoS): Impact on Sensors. 2018 4th International Conference on Information Management. Oxford, United Kingdom.