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

Maslina Daud[♣]
University of Malaya

Rajah Rasiah
University of Malaya

Mary George
University of Malaya

David Asirvatham
Taylor's University

Govindamal Thangiah
University of Malaya

ABSTRACT

Drawing on public goods and institutional theory, this study examines the mediation effect of cooperation on the relationship between organisational practices, namely, top management commitment (TMC), structured security processes (SSP) and security investment (SI) and cyber security compliance in organisations. Using data from Malaysia's critical sectors, ordinal regression was used to establish the odds of security compliance with security practices adjusted for job portfolio, security responsibility and educational levels. The results show that cooperation mediates TMC and SSP in achieving security compliance. The indirect effect of cooperation on these practices shows its subtle influence, which was not demonstrated in previous studies. These results also support the non-excludable characteristic of cyber security as a public good where cooperation overrides free-riding when security aspects are involved.

Keywords**:** Cooperation, Organisational Practices, Institutions, Security Compliance, Public Goods.

1. INTRODUCTION

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 spread of a piece of ransomware "Wannacry" in the recent cyber attack has swiped USD 4 billion within two weeks of the attack (Berr, 2017). The attack which affected 150 countries worldwide (Titcomb & McGoogan, 2017) did not spare Malaysia (Mohsen, 2017), and this was not the first time Malaysia experienced security breaches. In 2011, a hacker group calling themselves "Anonymous",

[♣]Corresponding author: Faculty of Economics and Administration, University of Malaya, 50603 Kuala Lumpur, Malaysia. Tel: +603 8992 6833 Email: maslina@cybersecurity.my

defaced 51 Malaysian government websites (BBC, 2011) citing that their actions were due to government restrictions imposed on the Internet (The Malaysian Insider, 2011). Based on the statistics produced by MyCERT, it has been an upward trend of cyber security incidents reported to them (CyberSecurity Malaysia, 2017).

The Wannacry attack that crippled businesses and government entities disclosed the weaknesses of how government and business sectors approached cyber security issues (Carlin, 2017) which non-compliant was identified as the main contributing factor of security breaches (Riordan, 2017). Thus, due to increasing dependence of technologies with the Internet as the core channel of communication, it is fundamental for organisations to adopt best practices in organisations to prevent breaches.

Previous security compliance models dealt with moulding employees behaviour through security policies, organisational and top management commitment (Bulgurcu, Cavusoglu, & Benbasat, 2010; Goo, Yim, & Kim, 2014; Kwon & Johnson, 2013). Fearlessness of prosecution (Straub Jr & Nance, 1990) and threat factor Johnston and Warkentin (2010) can orientate users to adhere to security practices in organisations. 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). Security scholars also pointed to other factors influencing compliance including knowledge sharing, collaboration, intervention and experience (Safa, Von Solms, & Furnell, 2016), continuous communication processes (Puhakainen & Siponen, 2010), information security climate (Goo, Yim, & Kim, 2014), formation of social bonds Ifinedo (2014) and attitude, normative beliefs, and self-efficacy (Bulgurcu, Cavusoglu, & Benbasat, 2010).

Although research on security compliance is abundant, little works exist on how cooperation contributes to security compliance. We argue that by mere understanding of human behaviour is not sufficient to understand how compliance is achieved in organisations. The underlying human behaviour factors that link organisational practices with security compliance need to be fully understood as organisational practices provide routines that can be followed by employees. Kostova (1999, p. 3) defined organisational practices 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. Since cybersecurity is everyone’s responsibility in organisations (Williams, 2008; Wylder, 2003), we hypothesize that cooperation is the underlying factor that influences organisational practices to strengthen security compliance. Thus, this study attempts to explore the mediation effect of cooperation on the relationship between organisational practices and security compliance. These effects can then serve as a baseline for organisations to consider practices in place and also provide insights for cyber security research. In this paper, three (3) organisational practices will be investigated, *viz.*, top management commitment, structured security processes and security investment. In doing so, this paper attempts to answer the following research question: What are the indirect effects of the relationship between top management commitment, structured security processes and security investment on cyber security compliance in organisations? Implicit in this question is the mediating role of cooperation.

Although the scope of this study are the Critical National Information Infrastructure (CNII) sectors in Malaysia, implications can also be drawn for other sectors from the results. The study deploys an empirical research design underpinned by the theory of Public Goods, which is ideal to understand how people cooperate in the common of interest of complying with cyber security. The rest of the paper is organised as follows. Section 2 discusses theories used in this study and section 3 presents the research model. This is followed by research methodology in section 4. Section 5 assesses and discusses the research results. Finally, section 6 finishes with the conclusions.

2. THEORETICAL CONSIDERATIONS

The important theories that deal with security issues are reviewed here. The purpose is to frame a cogent set of arguments on how economic agents can be motivated to cooperate so as to improve the conditions for security compliance. In so doing, the argument is also made to establish why cooperation is identified as an effective approach to achieve security compliance.

2.1. Public goods theory

From the perspective of public goods, people are the weakest link as these goods are non-excludable and non-rivalrous (Powell, 2005; Rosenzweig, 2012). Based on the underlying micro-economics principles, free-riding is the problem. The prominent characteristic of public goods, which is non-excludable to users provoke people to consume goods paying for it, and non-rivalrous, which allows people to continue consuming the same good without additional costs (Rosenzweig, 2012; Solum, 2010; Stigler, 1974). These 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.

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. However, characteristics of public goods also expose them to free-riding, which is also known as “failure of collective actions” as such benefits could also be enjoyed by free riders without contributing (Albanese & Van Fleet, 1985; Deneulin & Townsend, 2007). Due to its non-excludable characteristic, previous scholars (Burdett, 2003; Itoh, 1992) asserted that free-riding was associated with lack of cooperation among individuals in groups.

2.2. Cooperation theory

The evolution of cooperative behaviour is discussed extensively by Axelrod (1984). Using trade between two industrial nations an example, Axelrod (1984, p. 6) asserted that "the pursuit of self-interest by each through the introduction of trade barriers leads to a poor outcome for all." An example to demonstrate the benefits of cooperation can be shown through the "prisoner's dilemma" (Axelrod, 1984; Killingback & Doebeli, 2002; Trivers, 1971). In the prisoner’s dilemma case, two rational individuals opt not to cooperate simply because each of them lack the opportunity to initiate and forge cooperation. In examining various works related to cooperation, (Smith, Carroll, & Ashford, 1995, p. 10) concluded that cooperation is as a process in which individuals, groups and organisational interact and form relationship for mutual gain and benefit. Promoting cooperation in organisations allow a quick adaptation to changes such as innovative or technological changes in its environment (Schalk & Curşeu, 2010). An effective change management requires commitment by the top management to ensure compliance (Hu et al., 2012; ISO, 2013). Similarly, interdependencies from various business units demand cooperative efforts embedded in security processes. For example, incident management cannot be performed effectively when business units work in silos (Ahmad, Hadgkiss, & Ruighaver, 2012; Ahmad, Maynard, & Shanks, 2015). Whilst there was no clear evidence that associated cooperation with security compliance at organisational level yet, Tyran and Feld (2006), posited that in the legal domain, non-deterrent sanction such as self-imposed practices is capable to induce cooperation in complying with the law.

2.3. Institutional theory

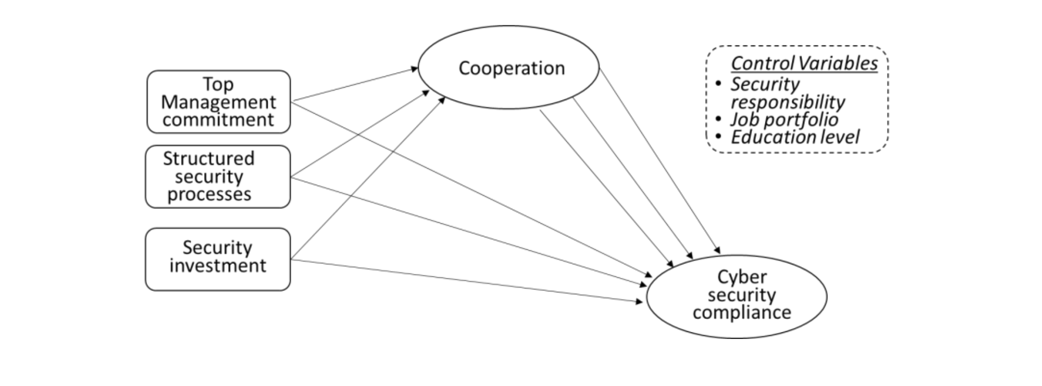
Role of institutions was discussed as a measure to avoid public goods from being abused (Hardin, 1968).Thus, we use North’s (1991) definition of institutions as the "rules of the game" and organisations as the "players" where capabilities of institutions are not only in forming up rules for societies and economies but also enforcing them in a formal or informal manner. 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. We also applied a neo-institutional theory that explains organisational change that can be influenced by three mechanisms; coercive, mimetic, and normative (DiMaggio & Powell, 1983). In this study, we focus only on coercive and mimetic mechanisms where coercive refers to pressure resulted from legislative related factors and mimetic explains how organisations tend to model themselves after others in similar population upon observing uncertainties in their environment. An example of mimetic is when organisations are pressured to imitate others due to benefits gained due to effective information security risks management (Steinbart et al., 2012). For CNII sectors in Malaysia, the Malaysian Government has taken a proactive approach for organisations in these sectors to implement Information Security Management System (ISMS) based on an international standard ISO/IEC 27001 and obtain certification (Bernama, 2010). Driven by a risk approach, this standard provides a holistic approach in managing cyber security by minimizing cyber security risks to an acceptable level and implementing relevant security controls.

3. RESEARCH MODEL AND HYPOTHESIS

This section focuses on the identification of variables, the research framework to gather the data and the hypotheses to test. This section also provides the justification for the variables selected and the framework to undertake the research.

Following the arguments reviewed from the above, we formulated a research model that comprises organisational security practices as key explanatory variables namely, top management commitment (TMC), structured security processes (SSP) and security investment (SI) and a single mediating variable cooperation (COOP) to achieve CSC in organisations (See Figure 1). The purpose of the research model is to capture both direct and indirect effects COOP has on these practices. These key explanatory variables were derived from two sources of isomorphic organisational change; coercive and memistic mechanisms which are discussed in the next subsections.

Figure 1: Research model


Top Management commitment
Structured security processes
Security investment
Cooperation
Cyber security compliance
Control Variables
• Security responsibility
• Job portfolio
• Education level

Source: Authors.

3.1. Cyber Security Compliance and Organisational Performance

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).

For this paper, in measuring organisational performance for CNII organisations, we use cyber security compliance achievement as the indicator. Adopting core safety activities at workplace by Griffin and Neal (2000) for safety compliance, we define cyber security compliance as cyber security requirements as core activities to be adhered by employees in meeting security objectives, where these requirements were embedded through policies and other related documents such as procedures, standards and legislations Wood (1997).

3.2. Cooperation

A study by Rodríguez, Pérez, and Gutiérrez (2008), suggests that cooperation was the only variable that was significant in achieving organisational performance through the success of their new products development. Management style that emphasized on affective commitment was capable of shaping employees' attitudes in obtaining cooperation (de Reuver & van Woerkom, 2010). Upon an extensive literature review, no previous studies that associated cooperation with CSC were found. However, for this study participation in organisational security initiatives is regarded as a proxy for cooperation where the influence of top management's participation in shaping employees' attitudes to comply with security policies was demonstrated (Hu et al., 2012; Vroom & Von Solms, 2004). In the context of public goods, Kaul, Grunberg, and Stern (1999) emphasized the importance of cooperation as an additional mechanism in ensuring that public goods to be adequately provided. Since a lack of cooperation contributed to free-riding behaviour (Burdett, 2003; Itoh, 1992), we argue that cooperation is the underlying factor contributing to compliance.

3.3. Top Management Commitment

TMC was studied due to mandate by the Government of Malaysia for CNII organisations to comply with the directive to implement Information Security Management System (ISMS) which is based on ISO/IEC 27001 standard. Referring this as coercive pressure, adherence with regulatory rules (Cavusoglu et al., 2015; Hu, Hart, & Cooke, 2007) has the effect for top management towards compliance (AlKalbani et al., 2016). TMC was also studied due to its significance on security performance in organisations (Kankanhalli et al., 2003; Knapp et al., 2006; Kritzinger & Von Solms, 2005; Kwon, Ulmer, & Wang, 2012) and its effect on compliance (Hu et al., 2012; ISO, 2013).

Previous security scholars asserted the importance of TMC in the forms of support (Knapp et al., 2006) and financial resources (Ramli, Mokhtar, & Aziz, 2014). Kankanhalli et al. (2003), demonstrated that organisations with better top management support engaged more in preventive security initiatives than those with the lesser support. Without top management support and involvement, security initiatives and efforts would have not been successfully implemented (Knapp et al., 2006; Kritzinger & Von Solms, 2005). 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). Focusing on procedural fairness and perceived charisma in motivating cooperation, leadership had an important role in influencing employees to cooperate (De Cremer & Van Knippenberg, 2002). However, these two factors were not examined in this study. Instead, committed leadership from the aspect of enforcement and provision of resources are the focus of this study.

Thus, we observe that the presence of cooperation is necessary in associating TMC with CSC and the following hypothesis is formulated:

H1: Cooperation has a mediating effect on the relationship between top management commitment and cyber security compliance

3.4. Structured security processes

Organisational processes should be structured and continuously improved to understand threats on changing technologies. Citing a discipline approach in software development, Batra (2010) suggested for processes to be structured, standardised and documented.

Adapting proactive and reactive definitions by (Baskerville, Spagnoletti, & Kim, 2014; Juhee & Johnson, 2014), we define proactive security process as processes that are to be developed and implemented with the objective to detect and prevent security breaches from occurring or reoccurring such as include risk assessment and business continuity (Järveläinen, 2013; Rocha Flores, Antonsen, & Ekstedt, 2014). Reactive processes are designed for security breaches to be responded to in a quick and effective manner (Ahmad, Hadgkiss, & Ruighaver, 2012; Line et al., 2008; Tøndel, Line, & Jaatun, 2014).

In complying with security requirements, these processes are necessary (Juhee & Johnson, 2014) since they comprise interdependence tasks that demand cooperation at all levels and interactions with internal and external counterparts. The higher task interdependence exist in groups the more importance of information sharing and other cooperative behaviours needed to complete those tasks (Thomas, 1957).

Therefore, we propose the following hypothesis:

H2: Cooperation has a mediating effect on the relationship between structured security processes and cyber security compliance

3.5. Security Investment

As organisations were pressured to comply with regulatory requirements, the level of investments were anticipated to increase in preventing security breaches (Cavusoglu et al., 2015). In establishing organisational security capabilities, investment should focus on both technology and non-technology aspects (Bonderud, 2016; Swarts, 2015). Organisations should not invest only in technology, but to embed people aspect in the process is fundamental to understand and make full sense of security technologies (Bonderud, 2016). In fact, employees' capabilities and competence have a positive effect on compliance Ifinedo (2014). However, a lack of formal components for technical implementations such as trainings and manuals may cause reluctance of employees to cooperate in implementing technical initiatives (Musa, 2012).

Thus, we propose the following hypothesis:

H3: Cooperation has a mediating effect on the relationship between security investment and security compliance

4. RESEARCH METHODOLOGY

This study is based on primary research as the Malaysian authorities or organisations have no past experience undertaking such a study. The data for this study was gathered through a survey that took account of all volunteers from the sampled organisations.

4.1. Instrumentation and Measurement

The questionnaire for data collection was arranged into two main parts. The first part consisted of demographic and basic information of respondents and the second part dealt with cyber security practices in the organisations. For this study, items of responses were measured on a five-point Likert scale, ranging from 1=Strongly disagree to 5=Strongly agree.

This study used a combination of single and multiple pieces of information to establish predictive validity of the measures. All variables in the study employed multiple-item scale or construct except COOP and CSC. Although certain scholars particularly in market research emphasized that results can be better achieved using multiple-items to measure (Churchill, 1979), there were arguments that value the level of acceptance of a single item measure. However, Bergkvist and Rossiter (2007, p. 183), 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". Although in most instances researchers are advised to deploy multiple-item scales (Churchill, 1979), single-item scales are still acceptable in certain circumstances (Diamantopoulos et al., 2012).

There are five variables used in this study mainly adapted from previous validated studies. We measured CSC by assessing the likelihood of respondents' organisations of achieving cyber security compliance with the presence of cooperation in organisations. For a clearer analysis, item's scores for CSC ranged from scale 1 to 5 were grouped into 3 categories where items "1" and "2" were grouped in category 1 (disagree), items "3" were grouped in category 2 (neither disagree nor agree), and finally items "4" and "5" were grouped in category 3 (agree). 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 senior management in information security and enforcement of security policies, procedures and other requirements in organisations. For this construct, respondents were asked to rate the commitment shown by their senior managements. We adopted this measure that was manifested in various forms; policy formulation and enforcement effectiveness by (Kwon, Ulmer, & Wang, 2012) and top management participation in security programmes by Hu et al. (2012). For the SSP, we adopted proactive focuses on risk (Yunos et al., 2014) and continuity (Aronis & Stratopoulos, 2016; Järveläinen, 2013) whereby reactive emphasizes the aspect of incident response and management (Ahmad, Hadgkiss, & Ruighaver, 2012; He, Johnson, & Lu, 2015). As for SI, we adopted security investment encompassing technologies, technical capabilities and practices (Juhee & Johnson, 2014; Liu, Tanaka, & Matsuura, 2008; Mulej, Rebernik, & Bradac, 2006). Technologies deployment requires human intervention through skills and expertise in manning them effectively. Thus, employees are more likely to comply with security policies when they have relevant competence in implementing security measures (Ifinedo, 2012).

In this study COOP serves as the mediator between TMC, SSP and SI and CSC. Established as a single item variable, it captures a high level of cooperation observed in organisations. A study by Rodríguez, Pérez, and Gutiérrez (2008), identified cooperation as a contributing factor to organisational performance. Thus, cooperation among employees in complying with security requirements is capable of minimizing opportunistic behaviour, eventually improve organisational performance in security.

In addition to the three explanatory variables, we also control for security responsibility level, job portfolio and educational level. Although (Wylder, 2003) argued that everyone is responsible to ensure information is protected and secure in organisations, there are groups of employees that are provided with roles and responsibilities to meet organisational security objectives e.g. top management, middle management and technical operations. While top management to provide resources and commitment, middle management has also been observed to bridge and serve other levels; top management, technical team and end users. Job portfolio was grouped into three categories, firstly, those that are responsible in ICT operations secondly, those that are responsible in security, and finally, those who are responsible in ICT planning, ICT risks and other related tasks. The final control variable is educational level which is grouped into three categories; degree, masters and phd.

4.2. Primary Data Collection

Under the National Cyber Security Policy (NCSP) ten (10) sectors have been identified as Critical National Information Infrastructure (CNII) sectors, viz., Government, Defense and Security, Finance and Banking, Information and Communication, Energy, Food and Agriculture, Transportation, Emergency Services and Health Services (Ministry of Science Technology and Innovation, July 2006). Primary data was collected using questionnaires from a sample of these organisations which are not geographically bound to particular location in Malaysia. There were approximately 200 organisations identified as CNII organisations. The education sector comprising of public and private universities was also included. Although universities are not directly listed under the CNII sectors, in cyber security, they are bound to be guided by the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) (National Security Council, 2012).

Purposive sampling, a non-probability sampling method was used in this study as it was important to identify and purposively seek information from organisations where cyber security is paramount. Allen (1971), posited that in deploying purposive sampling, it is crucial to source respondents who qualify as trusted informants in a study. Since information security background and knowledge are important in protecting organisational information assets (Rhee, Kim, & Ryu, 2009; Rocha Flores, Antonsen, & Ekstedt, 2014), these criteria became main criteria for choice of respondents who have critical roles in ensuring information security objectives are met.
220 questionnaires were distributed to respondents where 162 were collected, yielding a response rate of 73%. The questionnaires were distributed in 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).

Due to incomplete data, we dropped 7 observations leaving our final sample size to 155 which is higher than 150 as an acceptable sample size indicated by (Anderson & Gerbing, 1988).

4.3. Analytical Method

In analysing the results, mediation is opted as it is an approach where a researcher can 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).

For this study, the mediation effect of cooperation on the relationship between organisational practices and CSC was tested using the Karlson-Holm-Breen (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 induce the joint identification of co-efficient and error variances, which frequently occur in non-linear probability models. This statistical test allows the decomposition of total effect into direct and indirect effects in non-linear models (Kohler, Karlson, & Holm, 2011). Contrary to linear models that are quite straight forward, scaling problems occur in non-linear models as without mediating variables they frequently produce large standard error than models with mediating variables (Karlson & Holm, 2011). The KHB method rectifies this problem through rescaling which enables the comparison of the coefficients from both models (Karlson & Holm, 2011). 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.

5. RESULTS AND DISCUSSION

The results of the findings are examined in this section. The section first evaluates the descriptive and analytical statistics. It finishes with a discussion of the findings against the literature reviewed.

5.1. Descriptive statistics

The top three (3) respondents are those from the government (35.5%), education (20.0%), finance and banking and information and communication sectors (both are at 13.5%). Some responding organisations fit into two categories. For example, an organisation from the government sector can also be in the information and communication sector. Under such circumstances, the focus sector, i.e. the information and communication sector was preferred over the government sector. The respondents' demographic statistics are as in Table 1.

Table 1: Descriptive Statistics of the Respondents' Organisation

Description	Frequency, n (%)
Responsibility level	
Top management	23 (14.8)
Middle management	80 (51.6)
Technical operations	52 (33.5)
Job portfolio	
ICT operations	43 (27.7)
ICT Security	76 (49.0)
ICT Planning/Risk compliance/Others	36 (23.2)
Educational level	
Phd	19 (12.3)
Master	43 (27.7)
Bachelor and diploma	93 (60.0)
Year of service	
Less than 2 years	22 (14.2)
Between 2-5 years	28 (18.1)
Between 6-10 years	45 (29.0)
More than 10 years	60 (38.7)
Sector	
Government services	55 (35.5)
Defense and security	6 (3.9)
Finance and banking	21 (13.5)
Information and communication	21 (13.5)
Energy	4 (2.6)
Transportation	7 (4.5
Emergency services	1 (0.6)
Water	4 (2.6)
Health services	2 (1.3)
Food and agriculture	3 (1.9)
Education	31 (20.0)
Professional certification	
Professionally certified	56 (36.1)
No professional certification	99 (63.9)

Missing data was assessed where less than 10 percent missing data was detected in random fashion which is acceptable (Hair et al., 2010). The results of the internal consistency test show that the computed Cronbach value for variables are 0.6 and above. The Cronbach coefficient alpha values for measuring TMC (0.78), SSP (0.63) and SI (0.66) indicate acceptable reliability values (Moss et al., 1998). Although Cronbach's alpha internal consistency reliability value of 0.7 or higher is considered acceptable by (Gliem & Gliem, 2003; Nunnally, 1978) while Suhr and Shay (2009), suggested that 0.6 is acceptable if the analysis is for research purposes (Suhr & Shay, 2009). Several researchers have since used the 0.6 value (Setbon & Raude, 2010; Waljee et al., 2010). Regression models were later tested for multi-collinearity effect using Variance Inflation Factor (VIF). We estimated the VIF of all parameters and the statistics (1.00 – 1.90) were all below threshold of 10.0 which is acceptable (Marquaridt, 1970).

Table 2: Descriptive Statistics of the Variables Used in this Study

	n, (%)	Mean, (SD)	1 (n, %)	2 (n, %)	3 (n, %)
Cyber security compliance	155, (100%)	0.71, (0.45)	12, (7.74)	33, (21.29)	110, (70.96)
Top management commitment	155, (100%)	3.58, (1.19)	-	-	-
Structured security practices	155, (100%)	3.90, (0.53)	-	-	-
Security investment	155, (100%)	3.48, (0.63)	-	-	-
Cooperation	155, (100%)	1.89, (0.31)	-	-	-
Cooperative=1	139, (89.68%)	-	5, (41.67)	26, (78.79)	108, (98.18)
Non-cooperative=0	16, (10.32%)	-	7, (58.33)	7, (21.21)	2, (1.82)
Job Portfolio		1.95, (0.71)			
ICT operation	43, (27.7%)	-	4, (33.33)	12,(36.36)	27, (24.55)
ICT security	76, (49.1%)	-	4, (33.33)	9, (27.27)	63, (57.27)
Other ICT functions	36, (23.2%)		4, (33.33)	12,(36.36)	20, (18.18)
Responsibility level		2.18, (0.67)			
Top management	23, (14.84%)	-	2, (16.67)	6, (18.18)	15, (13.63)
Middle management	80, (51.61%)	-	6, (50)	16, (48.48)	58, (52.73)
Technical management	52, (33.55%)	-	4, (33.33)	11, (33.33)	37, (33.63)
Educational level		1.52, (0.71)			
Degree 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

Source: Computed from Authors Survey

The descriptive statistics of the variables used in this study were exhibited in Table 2 where statistics specific to TMC, SSP and SI and CSC were presented. We summarised the findings as follows. Firstly, 70.9% of the respondents agreed that CSC was achieved in their organisations followed by disagree category at 7.7% and neither of both at 21.3%. Secondly, in relation to agreeing that CSC was achieved, 98.2% of respondents of this category indicated that high cooperation level was observed in their organisations. This suggests that cooperation is positively related to CSC. Finally, the average response of all explanatory variables with standard deviation varies where TMC (mean=3.58, SD=1.19), SSP (mean=3.90, SD=0.53) and SI (mean=3.48, SD=0.63) indicating that SSP is the highest category of organisational practice embedded in organisations.

5.2. Statistical Analysis

Table 3 presents the mediation analysis results by the type of organisational practices after controlling for responsibility level, job portfolio and educational level. Two major findings were observed. Firstly, including COOP into the analysis significantly reduced the direct effects of two practices namely TMC and SSP towards 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 COOP was introduced. It shows that the co-efficient of TMC is statistically significant at 1% significance level and positive. This indicates that for every unit increase in TMC, the expected ordered log odds increases by 1.330 as CSC moves to the next higher category (that is from disagree to neutral and from neutral to agree) in achieving CSC, given all of other variables in the model are held constant. However, the magnitude reduced to 1.108 (direct effect) with OR=3.030 when COOP was included in the relationship. The difference of the magnitude which is 0.221 (indirect effect) represents the mediating impact that was statistically significant at 1% significance level and positive. Thus, H1 is supported.Similarly, there is also a positive mediating effect between SSP with CSC which is significant at 1% significance level where every unit increase in SSP, the expected ordered log odds increases by 1.440 as CSC moves to its next higher category. As COOP controlling the relationship, the effect of SSP reduces to 1.070, leaving an indirect effect of 0.441. Hence, H2 is supported.

However, the decomposition results show that the mediating effect on CSC by SI was not significant suggesting that there was no mediation effect that took place. Thus, H3 is not supported. However, it is worthy to note that the direct effect of this relationship is significant at 1% significance level and positive.

Table 3: The KHB Mediation Analysis by Organisational Practices and Cyber Security Compliance[a]

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)[b]	16.66%				
P_M (% of mediation)[c]	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)[d]	30.63%				
P_M (% of mediation)[e]	27.23%				
Security Investment (SI)[f]					
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
P_M (% of mediation)	n/a			0.473	1.231

Notes:

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

Source: Computed from Authors Survey

The importance of COOP is profound in both TMC and SSP. The overall results show that the inclusion of the COOP reduced magnitude of effects between TMC and SSP with CSC but not SI. The KHB test that calculated indirect effects (p=0.221 (TMC) and p=0.441 (SSP)) in the relationship after COOP was added to the model, confirming COOP as a mediator. The direct effect for both TMC and SSP remain significant after mediation indicating that partial mediation has taken place with the percent mediation (ratio of indirect effect to total effect) is P_M = 16.17 and P_M = 30.63 respectively.

Secondly, there was an effect of control variables in controlling the relationship. The results show a slight increase of the 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. Internalisation of normative pressures exerted on top management in these organisations through the ISMS directive requires top management to define, set and achieve security objectives in their organisation. The success in achieving the objectives is also very much dependent on commitment and enforcement. But, the effect is higher on SSP by 3.4% controlling by educational level and job portfolio. This was mainly due to more than half of the respondents hold the ICT security portfolio who are responsible to perform security tasks in ensuring security measures are in place. 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) who suggested that cooperative interactions were necessary when task interdependence involved. These findings are also supported by (Dzazali & 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, 2018) to 262 in 2017 (Department of Standards Malaysia, 2017). The increase also demonstrates the of mimetic isomorphism where other organisations follow the adoption of ISMS in CNII sectors in becoming risk averse organisations.

Thirdly, the insignificant of SI shows that cooperation was not obvious in getting security requirements to be complied with. Instead, SI was directly attributing to compliance which explains the significant roles of institutions in making it mandatory for CNII organisations to comply with ISMS which is driven by risk (Bernama, 2010).

5.3. Discussion

Our findings show that cooperation is the mediator in influencing employees to comply with organisational security requirements through cooperative efforts that were embedded in TMC and SSP. Contrary to previous studies where fear factor, threat appraisal, social bond and sanctions influence security compliance, this study provides evidence that cooperation through collective actions by employees contributed to CSC.

Previous studies have shown the impact of top management on employees' behaviour towards security compliance in organisations (Hu et al., 2012; Knapp et al., 2006; Kwon, Ulmer, & Wang, 2012; Puhakainen & Siponen, 2010). However, our study demonstrates that cooperation induced by senior management through instillation of a sense of belongings among employees can divert individual interests into more collective interests in working towards common goals. Supported by

Mulder, van Dijk, and De Cremer (2009), the likelihood for compliance to increase is largely dependent on how convincing the leaders are in encouraging cooperation in organisations.
Our findings on the significance of SSP are also supported by Rocha Flores, Antonsen, and Ekstedt (2014) where a process that was formally established and documented could coordinate security efforts. Processes should also be documented to allow those who are non-experts to conform to such processes (Batra, 2010). Our results are further supported by (Aronis & Stratopoulos, 2016; Holowachuk, 2007) where cooperation is crucial for IT department to work with other business units in rehearsing recovery procedures in preparation for disasters viz., cyberattacks. Exercising business and security procedures can promote cooperation in organisation through coordination, roles familiarisation and lessons learnt from periodic rehearsals. Ahmad, Hadgkiss, and Ruighaver (2012), stressed the needs for senior management, security and incident response teams to cooperate in negotiating priorities and determining actions while responding to security breaches. These were concurred by (Johnson, 2014; Line et al., 2008), that to recover from security incident, cooperation is required not only within the organisation, but also with external counterparts where interactions are crucial.

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. When the degree of interdependence is high, a mutual dependence is formed (Ramamoorthy & Flood, 2004) which 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.

6. CONCLUSION

Prior studies on security behavioural aspects particularly compliance have adopted several social theories to understand and conclude users' behaviour in information security domain. While those studies are important, we argue that in understanding the cyber security issue, the underlying characteristics of information security in a cyber ecosystem have not been really attended to. Thus, the results of this study provide evidence that in understanding cyber security problem, it should be investigated from the characteristics of the good itself.

The results of this study are also conclusive. Firstly, organisational practices through TMC and SSP are positively associated with CSC where this association is mediated by COOP through collective efforts in organisations. Although SI is not mediated through cooperation, it is positively associated with compliance. Secondly, tasks interdependencies in security processes demand cooperation in organisations through deployment of both proactive and reactive approaches that neither of them should be implemented in silos. Thirdly, 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 practices and 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.

This study also makes important contributions to theories. 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.

ACKNOWLEDGMENT

We would like to thank CyberSecurity Malaysia for providing their support for this study.

REFERENCES

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.

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.

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. J. (2016*). Investigating the Impact of Institutional Pressures on Information Security Compliance in Organizations.* Paper presented at the Australasian Conference on Information Systems 2016, Wollongong, Australia.

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

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

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.

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.

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

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.

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.

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

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.

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/

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/

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/

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

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.

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

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.

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

CyberSecurity Malaysia. (2017). *MyCERT Incident Statistics*. Retrieved from https://www.mycert.org.my/

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 Reuver, R., & van Woerkom, M. (2010). Can conflict management be an antidote to subordinate absenteeism? *Journal of Managerial Psychology, 25*(5), 479-494.

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

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.

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.

Dzazali, S., & Zolait, A. H. (2012). Assessment of information security maturity: an exploration study of Malaysian public service organizations. *Journal of Systems and Information Technology, 14*(1), 23-57.

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/

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.

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.

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 (7th Edition). Upper Saddle River: Pearson Higher Education.

Hardin, G. (1968). The Tragedy of the Commons. *Science, 162*(3859), 1243-1248.

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.

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.

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.

ISO. (2013). *ISO/IEC 27001:2013 Information Technology - Security techniques-Information security management systems-Requirements*. Retrieved from https://www.iso.org/

ISO/IEC27001. (2018). *ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements.* Retrieved from http://www.iso27001security.com/html/27001.html

Itoh, H. (1992). Cooperation in hierarchical organizations: An incentive perspective. *Journal of Law, Economics, & Organization, 8*(2),321-345.

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.

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.

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*.

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.

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., Grunberg, I., & Stern, M. A. (1999). Defining global public goods. *Global public goods: international cooperation in the 21st century,* 2-19.

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.

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.

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.

Kostova, T. (1999). Transnational transfer of strategic organizational practices: A contextual perspective. *Academy of management Review*, *24*(2), 308-324.

Kritzinger, E., & Von Solms, S. H. (2005). Five Non-Technical Pillars of Network Information Security Management. *Communications and Multimedia Security,* 277-287.

Kwon, J., & Johnson, M. E. (2013). Health-care security strategies for data protection and regulatory compliance. *Journal of Management Information Systems, 30*(2), 41-66.

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.

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. In R. Setola & S. Geretshuber (Eds.), *CRITIS 2008: Critical Information Infrastructure Security* (pp. 235-246). Berlin: Heidelberg Springer.

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.

MacKinnon, D. P., Fairchild, A. J., & Fritz, M. S. (2007). Mediation analysis. *Annual Review of Psychology*, *58*(1), 593-614.

Marquaridt, D. W. (1970). Generalized inverses, ridge regression, biased linear estimation, and nonlinear estimation. *Technometrics, 12*(3), 591-612.

Ministry of Science Technology and Innovation. (July 2006). *National Cyber Security Policy: The Way Forward*. Kuala Lumpur, Malaysia: Ministry of Science Technology and Innovation.

Mohsen, A. S. (2017, May 16). NSC releases advisory to ministries on WannaCry ransomware. *The Sun Daily*. Retrieved from http://www.thesundaily.my/

Moss, S., Prosser, H., Costello, H., Simpson, N., Patel, P., Rowe, S., & Turner, 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.

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* (Doctoral dissertation). University of Tasmania, Australia.

National Security Council. (2012). *Directive No. 24 National Cyber Crisis Management Mechanism and Policy*. Kuala Lumpur, Malaysia: National Security Council.

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.

Nunnally, J. C. (1978). *Psychometric theory*: McGraw-Hill New York.

Pais, J. (2014). Cumulative structural disadvantage and racial health disparities: The Pathways of childhood socioeconomic influence. *Demography, 51*(5), 1729-1753.

Pinsonneault, A., & Kraemer, K. (1993). Survey research methodology in management information systems: an assessment. *Journal of management information systems, 10*(2), 75-105.

Powell, B. (2005). Is Cyberspace a Public Good-Evidence from the Financial Services Industry. *Journal of Law Economics & Policy, 1*, 497-510.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly, 34*(4), 757-778.

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.

Ramli, A., Mokhtar, M., & Aziz, B. A. (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.

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.

Riordan, P. (2017). Most government agencies not compliant with cyber security controls. *The Australia*. Retrieved from http://www.theaustralian.com.au

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". 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.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

Schalk, R., & Curşeu, P. L. (2010). Cooperation in organizations. *Journal of Managerial Psychology, 25*(5), 453-459.

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.

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.

Solum, L. (2010). *Questioning Cultural Commons*. Cornell Law Review, *95*, 09-24. Retrieved from HeinOnLine database

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.

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.

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.

Suhr, D., & Shay, M. (2009). *Guidelines for reliability, confirmatory and exploratory factor analysis.* Proc. 2009 Western Users of SAS Conf. San Jose, CA.

Swarts, P. (2015, February 2). Obama budget dedicates $14B to cybersecurity. *The Washington Times.* Retrieved from http://www.washingtontimes.com

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

Thomas, E. J. (1957). Effects of facilitative role interdependence on group functioning. *Human Relations, 10,* 347-366.

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.

Trivers, R. L. (1971). The evolution of reciprocal altruism. *Quarterly review of biology*, *46*(1),35-57.

Tyran, J. R., & Feld, L. P. (2006). Achieving Compliance when Legal Sanctions are Non-deterrent. *The Scandinavian Journal of Economics, 108*(1), 135-156.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190-198.

Vieira, J. (2005). Water safety plans: methodologies for risk assessment and risk management in drinking-water systems. *IAHS-AISH Publication, 310,* 57-67.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191-198.

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.

Williams, P. A. (2008). In a 'trusting'environment, everyone is responsible for information security. *Information Security Technical Report, 13*(4), 207-215.

Wood, C. C. (1997). Policies alone do not constitute a sufficient awareness effort. *Computer Fraud & Security*, *1997*(12), 14-19.

Wylder, J. O. (2003). Improving security from the ground up. *Information Systems Security, 11*(6), 29-38.

Yunos, Z., Muhamad Pahri, N. a., Hashim, M. S., & Ahmad, R. (2014). Adoption of ISMS for Protecting SCADA Systems against Cyber Terrorism Threats. *International Journal of Computer and Information Technology, 03*(04), 819-822.