Journal of Palestine Ahliya University for research and studies
مجلـة جامعة فلسطين الأهلية للبحوث والدراسات
ISSN: 2959-4839
Vol. 03 Issue 02 (2024)

Top Management Leadership in Combating Information Security Threats through Organizational Information Security Practices

Qamarul Nazrin Harun✉*[1], Imran Harith Azmy[2], Nurhafizah Azizan**[1], and Abu Ubaidah Amir Abdul Aziz[3]

[1] College of Computing, Informatics, and Mathematics, Univesiti Teknologi MARA (UiTM), 85000, Segamat, Johor, Malaysia
*✉ qamarulnazrin@uitm.edu.my
**✉ nurha175@uitm.edu.my

[2] Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia (UTM), 54100, Kuala Lumpur, Malaysia
✉ Imranharithazmy@graduate.utm.my

[4] Universiti Geomatika, 54200, Kuala Lumpur, Malaysia
✉ abu@geomatika.edu.my

Received:05/03/2024 Accepted:25/03/2024 Published:01/08/2024

Abstract:

This study aims to examine the relationship between top management's role and information security practices (ISP) within Malaysian organizations and investigate the relationship between ISP and their effect on information security threats. A quantitative research design was used, and 352 questionnaires were collected from managers and executives of Malaysia Digital (MD)-status organizations in Malaysia. Structural equation modeling (SEM) was used to test all 18 hypotheses developed for this research. The results show that top management is highly associated with ISP in MD-status organizations, and the empirically-based framework developed in this research makes a significant contribution to the area of information security (InfoSec). The study highlights the importance of establishing an ISP that enlists the support of top management to lower the risk of information security threats and develop the organization's core principles. This research addresses the necessity for a thorough, coherent, and empirically verified Top Management Roles and ISP to reduce the risk of information security threats in Malaysian information technology (IT) companies.

Keywords: *Information Security; Management Leadership; Information Security Practices; Information Security Threat.*

دور القيادة الإدارية العليا في مكافحة تهديدات أمن المعلومات من خلال ممارسات أمن المعلومات التنظيمية

قمر الناظرين هارون✉[1*]، عمران حارث عزمي[2]، نور حفيظة عزيزان[1**]، أبو عبيدة أمير عبد العزيز[3]

[1] كلية الحوسبة والمعلوماتية والرياضيات، يونيفرسيتي تكنولوجيا مارا (UiTM)، 85000، سيغامَت، جوهور (ماليزيا)

qamarulnazrin@uitm.edu.my ✉[*]

nurha175@uitm.edu.my ✉[**]

[2] كلية رازك للتكنولوجيا والمعلوماتية، يونيفرسيتي تكنولوجيا ماليزيا (UTM)، 54100، كوالالمبور (ماليزيا)

Imranharithazmy@graduate.utm.my ✉

[3] يونيفرسيتي جيوماتيكا، 54200، كوالالمبور (ماليزيا)

abu@geomatika.edu.my ✉

تاريخ الاستلام:2024/03/05 تاريخ القبول:2024/03/25 تاريخ النشر:2024/08/01

ملخص:

تهدف هذه الدراسة للتعرّف على العلاقة بين دور الإدارة العليا وممارسات أمن المعلومات (ISP) داخل المنظمات الماليزية، والتحقق من العلاقة بين ISP وتأثيرها على تهديدات أمن المعلومات. تم استخدام المنهج الكمي، وتم جمع (352) استبانة من المديرين والمديرين التنفيذيين لمؤسسات الحالة الرقمية الماليزية (MD) في ماليزيا. وتم استخدام نمذجة المعادلة الهيكلية (SEM) لاختبار جميع الفرضيات الثمانية عشر التي تم تطويرها لهذا البحث. تظهر النتائج أن الإدارة العليا ترتبط ارتباطًا وثيقًا بمزود خدمة الانترنت في المؤسسات ذات الحالة الطبية، وأن الإطار القائم على التجربة الذي تم تطويره في هذا البحث يُقدّم إسهامًا كبيرة في مجال أمن المعلومات (InfoSec). وتسلط الدراسة الضوء على أهمية إنشاء مزود خدمة الإنترنت الذي يحصل على دعم الإدارة العليا لتقليل مخاطر تهديدات أمن المعلومات وتطوير المبادئ الأساسية للمنظمة. تكمن أصالة البحث بضرورة وجود أدوار إدارية عليا شاملة ومتماسكة ومثبتة تجريبيًا، وضرورة وجود مزودي خدمة الإنترنت لتقليل مخاطر تهديدات أمن المعلومات في شركات تكنولوجيا المعلومات الماليزية.

الكلمات المفتاحية: *أمن المعلومات؛ القيادة الإدارية؛ ممارسات أمن المعلومات؛ تهديد أمن المعلومات.*

1. Introduction

Organizations are highly dependent on the availability of information. The more information available within the organization, the more precise and realistic decisions can be made. Through information, organizations can set organizational direction, formulate long-term strategies, anticipate profits or losses in business, create an advantage over competitors, and create operational stability in the organization. Looking at the importance of the presence of information has made information the most valuable asset in the organization. Organizations that use information strategically can produce actions and decisions that benefit the organization. Looking at the value of the information found in the organization, it is enough to make the organization a target internally and externally. Organizational information that has been exploited risks putting the organization in danger. Cybercriminals can carry out various attacks based on the information they obtain from the organization, causing the organization to spend a lot of resources to repair the damage that has occurred in the organization. In addition to the organization's image and reputation being damaged, investors will no longer be interested in investing in the organization. Despite the critical role of information in organizations, the theoretical underpinnings that describe how top management's engagement with Information Security Practices (ISP) impacts an organization's resilience to cyber threats are notably sparse. Existing research, such as the works by Alhogail and Mirza (2014), Alkabani et al. (2014), Martins and Veiga (2015), has begun to sketch the outline of organizational information security culture and practices. However, these studies often do not leverage or develop theoretical frameworks that explicitly detail the casual pathways through which top management influences information security outcomes. This leaves a significant gap in our understanding of the mechanisms at play, particularly in how top management's strategic commitment to ISPs can fortify organizational defenses against increasingly sophisticated information security threats. This study aims to bridge this theoretical divide by proposing a nuanced exploration into the direct and indirect effects of top management's engagement with ISPs, seeking to both delineate and empirically validate the theoretical constructs that govern these relationships.

ISP among employees at all levels can create a safe and alert environment against any attempted information intrusion in the organization. Through effective ISP, employees are equipped with the knowledge and preparation to deal with various information security threats. Organizations that do not implement ISP effectively will lead workers to not know what measures should be performed if the organization encounters a threat to information security, resulting in serious damage to information assets and the organization being at a loss.

Management is in charge of establishing information security protocols throughout the organization. Management is the backbone of the organization. Through management, the direction and work culture in the organization can be set. Management is also a prime role model that employees can follow. The commitment of management in establishing a safe work environment can create a safe environment in the organization. Although many studies touch on the aspects of management's role in smoothing operations in organizations (Kwon et al., 2013; Yoo, 2014; Masrek et al., 2019), few studies focus on the role of the organization's top management in creating holistic ISP in organizations. This oversight becomes particularly critical in light of the rapidly evolving landscape of information security threats, which continues to present a dynamic challenge to organizational resilience. The nature of these threats, which evolve alongside technological advancements, necessitates a more agile and informed response strategy, one that is deeply influenced by the proactive engagement and motivation of top management. At the same time, the development of information security threats that are constantly changing over time has further increased the risk of organizations in dealing with information security threats. If highlighted, even though technology is growing, organizations are still faced with information security threats that cause a lot of damage and losses in the organization. This shows that in addition to technology, organizational information security behavior is also the main factor that must be seen to protect information assets in the organization (Metalidou et al., 2014). This behavior can be seen through human resources in the organization through ISP. The question is, does top management motivation affect ISP in the organization in a major way? And do ISP affect information security threats to the organization?

The objectives of this research are (i) to assess the relationship between top management's role and ISP within an organization and (ii) examine the relationship between ISP and their effect on information security threats in organizations.

This article's management is structured as follows: The literature is discussed in Section 2 along with the creation of research models and hypotheses. Section 3 addresses research methodology. Section 4 of the article discusses the emphasis on empirical results. Finally, researchers conclude the study in sections 5 and 6 by concentrating on the discussion of research's contributions and implications.

2. Literature Review and Theoretical Framework

According to Diesch et al. (2020), considering information security as a purely technical matter and merely allocating technical workers to information security tasks has proven ineffective. The confidentiality, integrity, and availability of information are at the heart of every information security strategy. Nieles et al. (2017) noted that confidentiality is "the preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information," whereas integrity is "the prevention of improper information modification or destruction, as well as the assurance of information non-repudiation and authenticity". The availability of information is concerned with assuring prompt and dependable access to and use of information. Efforts to ensure confidentiality, integrity, and availability are always protected from information security threats, and they need to involve not only technical factors but also important humanitarian factors. Nowadays, information security threats are not only targeted at technological weaknesses. Metalidou et al. (2014) found that human weakness is the main target of cybercriminals to commit various crimes. Resent theoretical models, such as the integrated framework proposed by Liang et al. (2017), emphasize the interplay between technical and human factors in shaping effective information security environments, suggesting a more nuanced understanding of how organizational practices mediate these influences.

Information security threats are described as "any possible harm to computers and network resources, such as illegal access to private information, virus infection, and system failure" (Bace, 2000). Information threats are regarded as gaining specific information, which is usually sensitive and secret information of certain companies and people. External threats are presented by outsiders, whereas internal threats are posed by those working inside organizations. External threats seem to be more serious than internal ones (Al-Mhiqani et al., 2020). Internal threats were described by Al-Awadi and Renaud (2007) as "misuse of computer access controls; harm caused by a disgruntled employee; installation or use of unauthorized hardware, peripherals; actual theft of unauthorized hardware or software; human error; use of unauthorized software; and use of organization resources for illegal communications or activities (porn surfing, email harassment)". Jouini et al. (2014) argued that both internal and external sources might pose information security threats. The goal of an attacker on a system may often be malicious or benign, but the reason for why the threat is created can either be intentional or unintentional.

Some of the effects that might follow from an information security threat include information destruction, information corruption, information theft/loss, information disclosure, denial of use, privilege elevation, and illegal use. Ernst and Young (2018) defined the information security threat landscape into three categories: common, advanced, and emergent. The most prevalent kind of attack is one carried out by a beginner utilizing publicly accessible hacking tools to exploit known flaws. The developing category includes assaults carried out by professionals who concentrate on vectors and weaknesses allowed by new technologies that have been found via a particular study.

ISPs play a very important role in ensuring that the information environment is always away from the risk of information security incidents. Information Security Management Standards (ISMS), such as ISO/IEC 27001 and ISO/IEC 27002, have been developed to ensure that organizational ISPs can be monitored in a structured manner and reduce the risk of information security threats occurring within the organization. According to Hsu and Wang (2015), in order to retain organizational assets, top management must be involved in and responsible for establishing the boundaries of risk management. Top management commitment often results in moral and financial support for the adoption of information security. As a consequence, the implementation of information security measures would almost certainly fail without the dedication and participation of top management. The conceptual model by Chang and Lin (2015) further delineates how top management's commitment to information security practices enhances organizational resilience, serving as a theoretical underpinning for examining the mediation effect of ISPs on information security threat mitigation.

To examine the impact of top management, Kankanhalli et al. (2003) conducted research on information systems managers from diverse economic sectors. The results showed that companies with strong top management guidance took more preventative measures than companies with less effective top management support. Kazemi et al. (2012) conducted research on information security practices in Iranian municipal organizations. The study also found that senior management support, namely management commitments, responsibilities, and understanding of information security, was crucial in developing an information security culture. The results indicated that social pressure, information security expertise, management commitments, and accountability all had a strong beneficial influence on information security compliance in organizations. Building on the contingency theory, which posits the need for alignment between organizational strategy and environmental demands, Zhou et al. (2016) provide a theoretical basis for understanding the critical role of top management's support in developing adaptive information security strategies.

A study was undertaken by Kwon et al. (2013) to assess the correlation between the number of information security breaches and the participation of IT executives on the organization's top management team. According to the findings of their research, the number of information security breaches greatly decreased when IT executives actively participated and played a role in providing advice to the organization's top management team. Although the senior management team in an organization often comes from a variety of professional backgrounds, this does not always mean that they will have the greatest levels of motivation and attention when it comes to the protection of the organization's information assets. As a result, it is believed that the presence of IT executives in this group may have an impact on the organization's top management, which in turn can draw the top management's attention to security standards and principles, as proven empirically through this study. Through easier communications and across departments, it also influences security management behavior. The organization's environment may be protected from the risk of information security breaches via good coordination of the top management and employee adherence to the information security policy.

Yoo (2014) performed a survey with 1,035 firms from diverse industries. His research aimed to examine how the organization's top management's leadership in information security might affect information security control throughout the organization. Information security policy, organizational structure, organizational responsibility, information security awareness and training, technical measure installation and operation, emergency response, monitoring, and auditing toward information security are all included in Yoo's concept of information security controls. According to this research, the level of information security leadership within an organization may directly affect how effectively information security controls are implemented, lowering the risk of information security risks within the organization.

Masrek et al. (2019) conducted an empirical study with the aim of evaluating the role of top management in influencing ISP, involving 292 respondents representing agencies in Malaysian public organizations. The results of their study showed that all hypotheses were accepted. This means that the top management consisting of information security commitment and information security importance has the ability to shape the effective ISP in the organization. The research model proposed by them involved information security policy effectiveness, information security directives, and information security responsibility as dependent factors that determine ISP in organizations.

The research model represented in Figure 1 was developed based on the findings stated above. In this research, the independent variable is top management, which has two dimensions: information security commitment (ISC) and information security importance (ISI). These dimensions were derived from the work of Flores et al. (2014), Martins and Da Veiga (2015), Masrek et al. (2018), and Kudjo et al. (2017). The moderating variable is organizational ISP, which includes six dimensions: information security knowledge sharing (ISKS), information security education (ISE), information security visibility (ISV), information security policy effectiveness (ISPE), information security responsibility (ISR), and information security directives (ISD). To explore the mechanisms through which top management's ISC and ISI dimensions influence organizational ISPs and, in turn, impact the organization's resilience to information security threats, this study posits the existence of a mediation effect within this relationship. All ISP dimensions are then linked to information security threats as a dependent variable. Specifically, this mediation effect is hypothesized to operationalize through the enhanced information security culture and practices that stem from effective top management commitment and strategic importance placed on information security. Accordingly, the study introduces the following hypotheses: H1: Higher levels of top management's information security commitment and information security importance are positively related to organizational ISPs. H2: Organizational ISPs mediate the relationship between top management's information security commitment and importance and the organization's resilience to information security threats. The operational definitions for the variables and research hypotheses are presented in Table 1. The work of Masrek et al. (2018) served as the foundation for each definition.

Building upon the theoretical underpinnings provided by these foundational studies, additional insights from the Socio-Technical Systems theory suggest that the interdependencies between social and technical aspects within organizations play a crucial role in the effective management of information security practices. This theory supports the notion of ISPs as a mediator by illustrating how organizational culture and top management's strategic orientation towards information security can significantly influence the efficacy of technical security measures. Furthermore, the Technologi-Organization-Environment (TOE) framework offers a valuable perspective on how external environmental factors, organizational characteristics, and technological capabilities converge to shape an organization’s approach to information security management, reinforcing the importance of examining ISPs within the context of top management’s strategic decisions. These theoretical perspectives enrich the study’s examination of the mediation effect and underscore the complexity of relationships between top management, organizational ISPs, and the mitigation of information security threats.

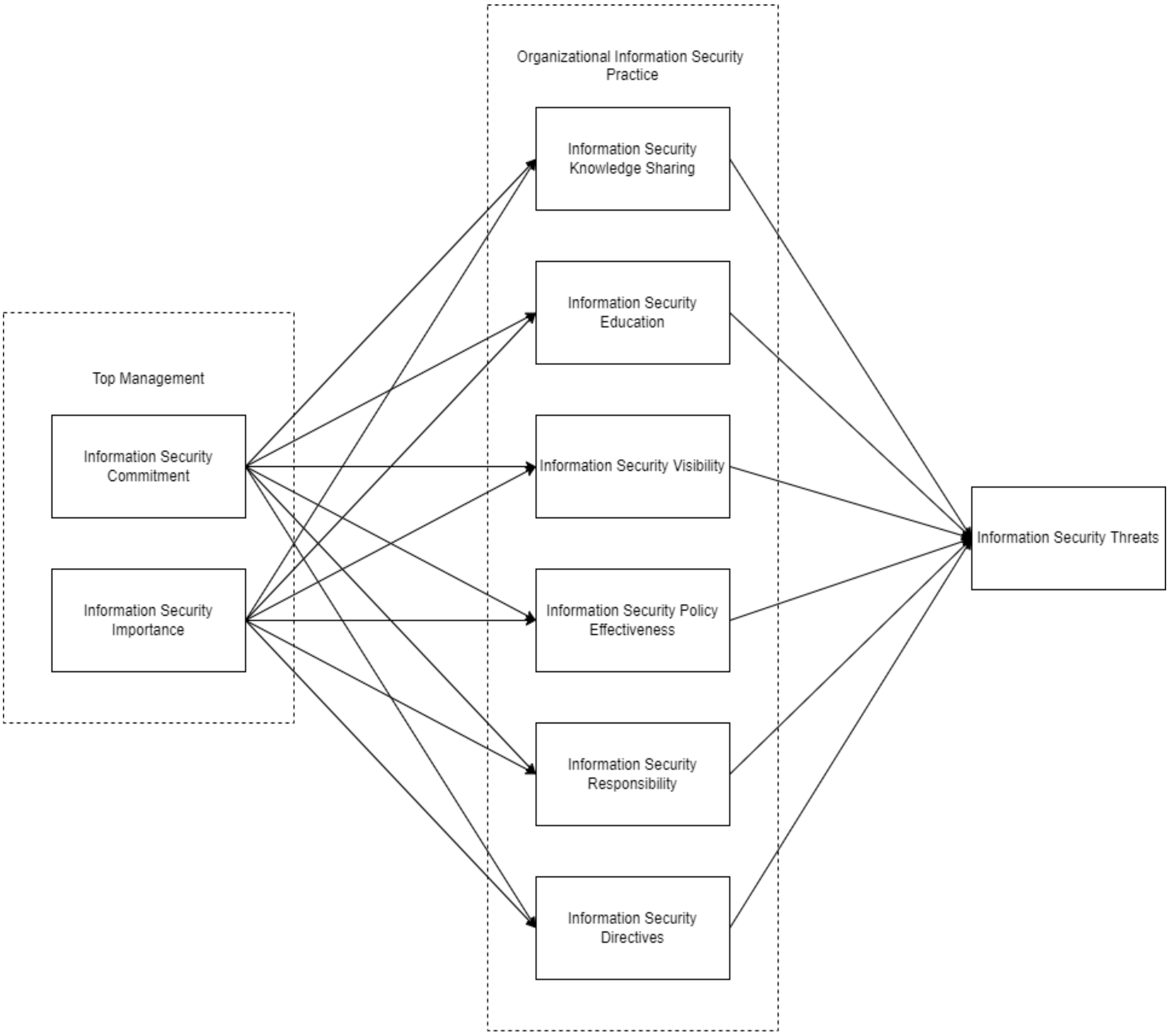
Organizational Information Security Practice
Information Security Knowledge Sharing
Information Security Education
Top Management
Information Security Commitment
Information Security Visibility
Information Security Threats
Information Security Importance
Information Security Policy Effectiveness
Information Security Responsibility
Information Security Directives

Figure 1: Research Model

Table 1: Operational Definitions and Hypotheses

Construct	Operational Definition	Hypothesis
Information Security Commitment	“The extent to which top management fully supports and participates in an organisational information security initiative”	Not applicable
Information Security Importance	“The extent to which top management prioritises information security above other tasks”	Not applicable

Information Security Knowledge Sharing	“The readiness of people, organisations, or groups to impart or disseminate information security expertise to others”	H1: Information Security Knowledge Sharing is significantly predicted by Information Security Commitment H2: Information Security Knowledge Sharing is significantly predicted by Information Security Importance
Information Security Education	“By adopting academic teaching techniques, an effort is made to ensure that every employee has the information security skills and knowledge needed to secure organisational information”	H3: Information Security Education is significantly predicted by Information Security Commitment H4: Information Security Education is significantly predicted by Information Security Importance
Information Security Visibility	“The extent to which an organisation makes an attempt to give employees a favourable impression of information security policy”	H5: Information Security Visibility is significantly predicted by Information Security Commitment H6: Information Security Visibility is significantly predicted by Information Security Importance
Information Security Policy Effectiveness	“The evaluation of the information security policy, including whether it is clear, applicable, and effectively conveyed”	H7: Information Security Policy Effectiveness is significantly predicted by Information Security Commitment H8: Information Security Policy Effectiveness is significantly predicted by Information Security Importance
Information Security Responsibility	“The person or organisation in charge of ensuring that information security regulations are followed”	H9: Information Security Responsibility is significantly predicted by Information Security Commitment H10: Information Security Responsibility is significantly predicted by Information Security Importance
Information Security Directives	“The explicit guidance or instruction on guarding against information security events, such as information security breaches perpetrated by unauthorised parties”	H11: Information Security Directives is significantly predicted by Information Security Commitment H12: Information Security Directives is significantly predicted by Information Security Importance
Information Security Threats	“Information security breaches or threats that are mostly caused by untrustworthy and unauthorised persons or groups, whether inside or outside over the organisation”	H13: Threats to information security are negatively correlated with information security knowledge sharing. H14: Threats to information security are negatively correlated

	with information security education. H15: Threats to information security are negatively correlated with information security visibility. H16: Threats to information security are negatively correlated with information security policy effectiveness. H17: Threats to information security are negatively correlated with information security responsibility. H18: Threats to information security are negatively correlated with information security directives.

3. Research Methodology

In line with Noordin and Masrek's (2016) suggestions, a survey research technique was used. The data was gathered via a questionnaire that was answered via an online form. The researcher constructed most of the questionnaire items. There were 56 items in the questionnaire's first draft. Six items were used for each construct. A Likert scale with five anchors was applied to each item. Each item's anchoring was situated halfway between the extremes of "1 = not practiced at all" and "5 = highly practiced". This was done to determine the degree to which the specified items were implemented in the respondents' organizations.

The questionnaire was pre-tested and pilot-tested with a number of subject matter experts, including academics and business professionals, prior to the primary data collection. The questionnaire was revised in response to their comments and recommendations. A pilot test was carried out after the pre-test exercise. The exercise involved engaging 353 IT managers who worked at MD-status enterprises. To assess the reliability for each construct, the responses of this study were calculated using Cronbach's Alpha. The findings demonstrated that all construct scores were significantly higher than 0.7, indicating that the questionnaire was reliable for use in the research.

Since a firm or organization served as the study's unit of analysis, the population must be a list of such entities. The InforTech cluster of MD-status organizations, which consists of 1189 companies, was selected as the study's population. This research employed a convenient sampling strategy and mailed 420 questionnaires to the IT managers of these companies, representing approximately 35% of the InforTech cluster. These IT managers were asked to reply on behalf of the company to the questionnaire. At the end of the data collecting period, 352 were returned and determined to be appropriate for further study, constituting an 83.8% response rate from the sampled population and providing a substantial cross-section for analysis.

In this study, partial least square structural equation modeling (PLS-SEM) was used to examine the research data. The SEM analysis consisted of two steps: Confirmatory factor analysis (CFA), often known as the assessment of the measurement model, and the evaluation of the structural model. The measuring model was evaluated for convergent and discriminant validity.

Contrary to discriminant validity, which is concerned with how much the items differ across constructs, convergent validity is concerned with how similar the items are in evaluating the constructs. Normally, structural models are used to evaluate hypothesis connections between constructs. The stages involved in evaluating structural models are as follows: (i) the evaluation of collinearity concerns, (ii) the evaluation of the importance and relevance of the structural model relationship, (iii) the evaluation of the coefficient of determination (R^2), (iv) the evaluation of impact size (f^2), and (v) the evaluation of predictive relevance (Q^2).

4. Findings

4.1 Common method bias

Common method bias poses a serious risk to studies that only use one data source and could impair the validity of the findings (Podsakoff & Organ, 1986). Therefore, the Harman's single factor test was carried out to determine whether such a threat existed in the dataset. In order to examine all items from all constructs, only a single factor was allowed. The findings revealed that only 48.46% of the total variance could be attributed to a single factor, falling just short of the cut-off point of not more than 50%. These findings indicated that there were no obvious signs of common method bias in the data that was gathered.

4.2 Demographic profiles

The IT manager was asked to respond on behalf of the MD status organisations as the firm or organisation served as the study's unit of analysis. In terms of gender, 50.5% were men and 49.5% were women, those responded to the survey. The respondents' age range was as follows: 32.4% are between the ages of 41 and 45, 28.6% are between the ages of 36 and 40, 11% are between the ages of 26 and 30, 10.5% are between the ages of 46 and 50, 9.8% are between the ages of 16 and 20, 10.5% are between the ages of 6 and 10, 10.2% are between the ages of 1 and 5, and 9.8% are between the ages of 26 and 30. In terms of years of service, 23.3% indicated they had served between 21 and 25 years, 21.9% between 11 and 15 years, 16.1% between 16 and 20 years, 10.5% between 6 and 10 years, 10.2% between 1 and 5 years, and 6.2% had served for more than 30 years.

4.3 Measurement model

The findings of the convergent validity evaluation of the measurement model are shown in Table 2. As 29 items had to be deleted owing to poor factor loading, there were 27 items left to measure information security threats. Factor loading, composite reliability (CR), and average variance extracted (AVE) were the measures used to evaluate convergent validity. In accordance with the literature, the factor loading should be more than 0.700, however values of 0.4, 0.5, and 0.6 are acceptable in some situations (Ramayah et al., 2018). The acceptable values for CR and AVE were respectively at least 0.7 and 0.5. All of these conditions appeared to be satisfied based on the data shown in Table 2, which suggests that convergent validity may be assumed.

Table 2: Assessment of Measurement Model

Construct	Item Code	Item Statement	Factor Loading	Composite Reliability	Average Variance Extracted (AVE)
Information Security Commitment	ISC2	"Top management that is supportive to information security policy enforcement"	0.8	0.853	0.659
	ISC5	"Top management that is dedicated to increasing employee's awareness regarding information security"	0.816		

	ISC6	“Top management that provides mentoring and training opportunities regarding information security”	0.82		
Information Security Directives	ISD3	“Clear directives regarding information sharing within and outside the organisation”	0.807	0.854	0.66
	ISD5	“Clear directives on the prevention of information security breaches”	0.828		
	ISD6	“Clear directives for the compliance of organisation’s policy and procedures”	0.802		
Information Security Education	ISE1	“Organisation provides employees with appropriate security education before giving them authorised access to the corporate network”	0.814	0.86	0.672
	ISE5	“Organisation provides employees with education on the steps to be taken in the event of an information security incident”	0.814		
	ISE6	“Organisation provides employees with information security awareness education to all employees regardless of position in the organisation”	0.831		
Information Security Importance	ISI1	“Top management that gives significant priority for information security policy establishment”	0.822	0.863	0.677
	ISI4	“Top management that reacts immediately when there are information security breaches”	0.823		
	ISI5	“Top management that educates employees on the importance of information security enforcement”	0.823		
Information Security Knowledge Sharing	ISKS1	“Employees frequently share their experiences about information security”	0.816	0.864	0.679
	ISKS3	“Employees frequently talk with others about information security incidents and their solutions”	0.83		
	ISKS6	“Employees frequently share precautionary measures to prevent information security incidents”	0.826		
Information Security Policy Effectiveness	ISPE2	“The information security policy that is practical to be applied by employees irrespective of their ranks”	0.814	0.865	0.681
	ISPE5	“The information security policy that ensures regulatory compliance with various privacy and security laws”	0.826		
	ISPE6	“The information security policy that is regularly reviewed and updated”	0.835		

Information Security Responsibility	ISR1	"Entrusting the employee with responsibility for the protection of organisational resources"	0.793	0.846	0.647
	ISR2	"Clearly defining roles and responsibilities of each employee regarding ISP"	0.818		
	ISR6	"Involving employee in the formulation of information security policy"	0.802		
Information Security Visibility	ISV1	"Information security activities are widely advertised in organisation"	0.813	0.893	0.736
	ISV2	"Information security incidents are visible publicly in organisation"	0.834		
	ISV4	"Information security training is widely advertised in organisation"	0.807		
Information Security Threats	IT3	"Employees accidentally send inappropriate email messages"	0.857	0.859	0.669
	IT6	"Former employees use organisational computer systems to carry out financial fraud or theft"	0.85		
	IT8	"Employees fall trap to phishing emails"	0.867		

After determining the convergent validity, the Fornell and Larcker (1981) discriminant validity measure was carried out. When the square root of the AVE is greater than the correlations between the construct and other constructs, discriminant validity may be inferred. The results in Table 3 strongly imply that the requirements were fully satisfied, indicating that the discriminant validity of the model may be accepted. Figure 2 depicts the output of the SmartPLS of the measurement model.

Table 3: Fornell and Larker (1981) Assessment of Discriminant Validity

	ISC	**ISD**	**ISE**	**ISI**	**ISKS**	**ISPE**	**ISR**	**IST**	**ISV**
IS Commitment (ISC)	0.812								
IS Directives (ISD)	0.747	0.813							
IS Education (ISE)	0.714	0.737	0.82						
IS Importance (ISI)	0.722	0.723	0.683	0.823					
IS Knowledge Sharing (ISKS)	0.74	0.746	0.753	0.708	0.824				
IS Policy Effectiveness (ISPE)	0.706	0.743	0.719	0.722	0.702	0.825			
IS Responsibility (ISR)	0.731	0.744	0.727	0.719	0.72	0.722	0.805		
IS Threat (IST)	-0.781	-0.775	-0.774	-0.756	-0.767	-0.756	-0.769	0.858	
IS Visibility (ISV)	0.726	0.718	0.743	0.711	0.685	0.695	0.72	-0.757	0.818

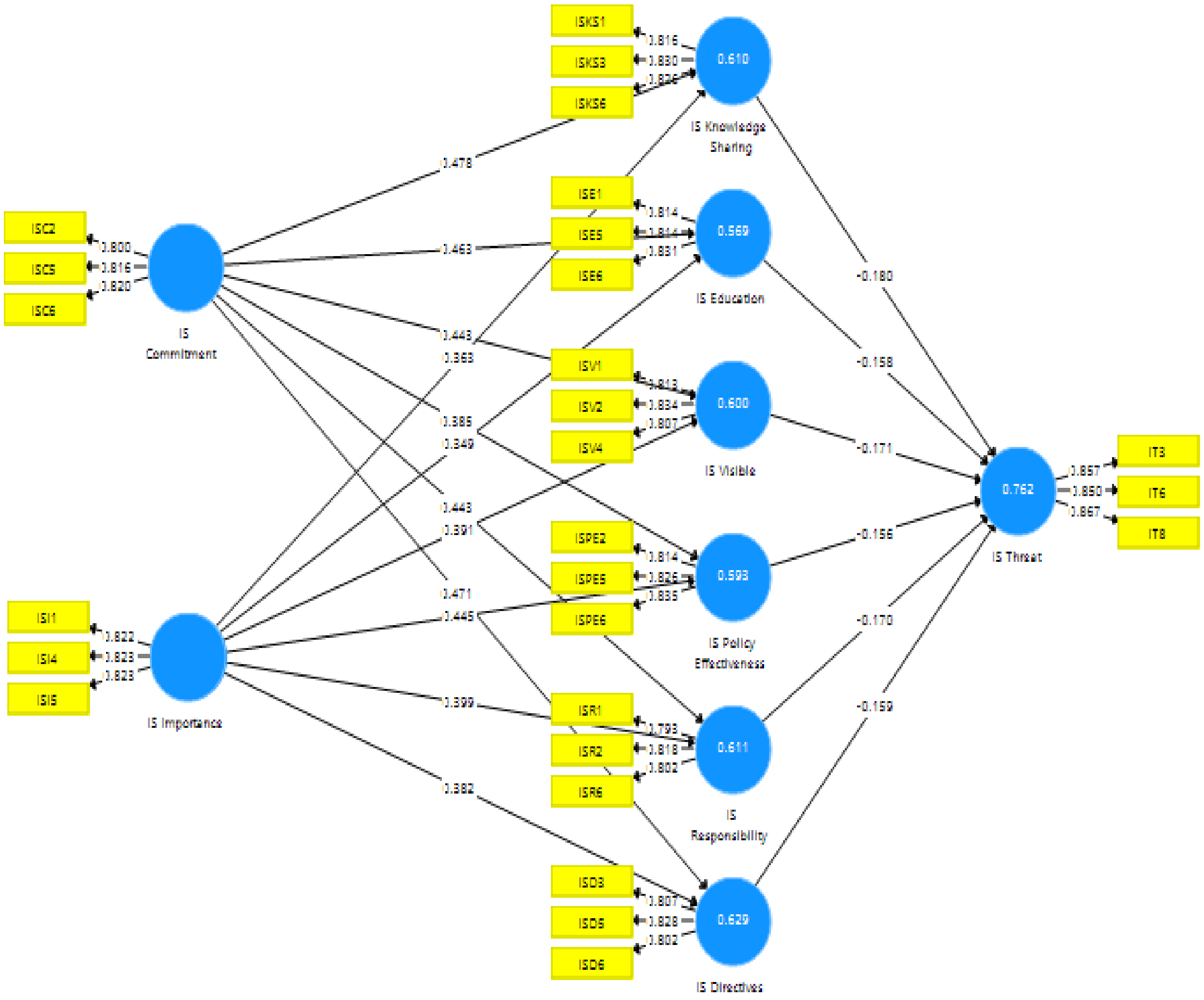

Figure 2: SmartPLS Output of the Measurement Model

4.4 Structural model

Variance inflation factors (VIF) values of 3.3 or above are indicative of a potential collinearity issue (Diamantopoulos & Siguaw, 2006). None of the VIF scores exceeded 3.0 or 5.0, according to the findings, indicating that multicollinearity problems were not present in the data.

Table 4 displays the results of the hypothesis testing. Every relationship between independent factors and dependent variables was significant, with t-values ranging from 3.593 to 12.302 ($p < 0.001$). Above the Falk and Miller (1992) suggested the cut-off point of 0.10, the R^2 values for the relationship between independent and dependent variables varied from 0.569 to 0.762. Cohen (1988) defined the effect sizes of f^2 values of 0.35, 0.15, and 0.02 as high, medium, and small, respectively. All paths in this research had either small or moderate f^2 values.

The structural model was tested for predictive relevance according to the literature using the Stone-Geisser's Q^2 test (Stone, 1974; Geisser, 1974). The findings revealed that all dependent variable Q^2 scores were significantly above zero, suggesting that the model has predictive value. Figure 3 displays the structural model's output from SmartPLS.

Table 4: Results of Hypothesis Testing

	R^2	Std Beta	Std Error	T Value	P Value	f^2	Q^2	Decision
IS Commitment -> IS Knowledge Sharing	0.61	0.478	0.039	12.302	0	0.28	0.409	Accepted H1
IS Importance -> IS Knowledge Sharing		0.363	0.039	9.18	0	0.161		Accepted H2
IS Commitment -> IS Education	0.569	0.463	0.046	9.96	0	0.238	0.377	Accepted H3
IS Importance -> IS Education		0.349	0.048	7.333	0	0.135		Accepted H4
IS Commitment -> IS Visibility	0.6	0.443	0.039	11.268	0	0.235	0.395	Accepted H5
IS Importance -> IS Visibility		0.391	0.043	9.202	0	0.183		Accepted H6
IS Commitment -> IS Policy Effectiveness	0.593	0.385	0.04	9.603	0	0.174	0.398	Accepted H7
IS Importance -> IS Policy Effectiveness		0.445	0.043	10.46	0	0.232		Accepted H8
IS Commitment -> IS Responsibility	0.611	0.443	0.041	10.845	0	0.242	0.391	Accepted H9
IS Importance -> IS Responsibility		0.399	0.04	10.108	0	0.197		Accepted H10
IS Commitment -> IS Directives	0.629	0.471	0.038	12.298	0	0.286	0.411	Accepted H11
IS Importance -> IS Directives		0.382	0.04	9.492	0	0.188		Accepted H12
IS Knowledge Sharing -> IS Threat	0.762	-0.18	0.044	4.115	0	0.045	0.553	Accepted H13
IS Education -> IS Threat		-0.158	0.039	4.011	0	0.031		Accepted H14
IS Visibility -> IS Threat		-0.171	0.038	4.444	0	0.043		Accepted H15
IS Policy Effectiveness -> IS Threat		-0.156	0.037	4.263	0	0.035		Accepted H16
IS Responsibility -> IS Threat		-0.17	0.044	3.883	0	0.039		Accepted H17
IS Directives -> IS Threat		-0.159	0.044	3.593	0	0.032		Accepted H18

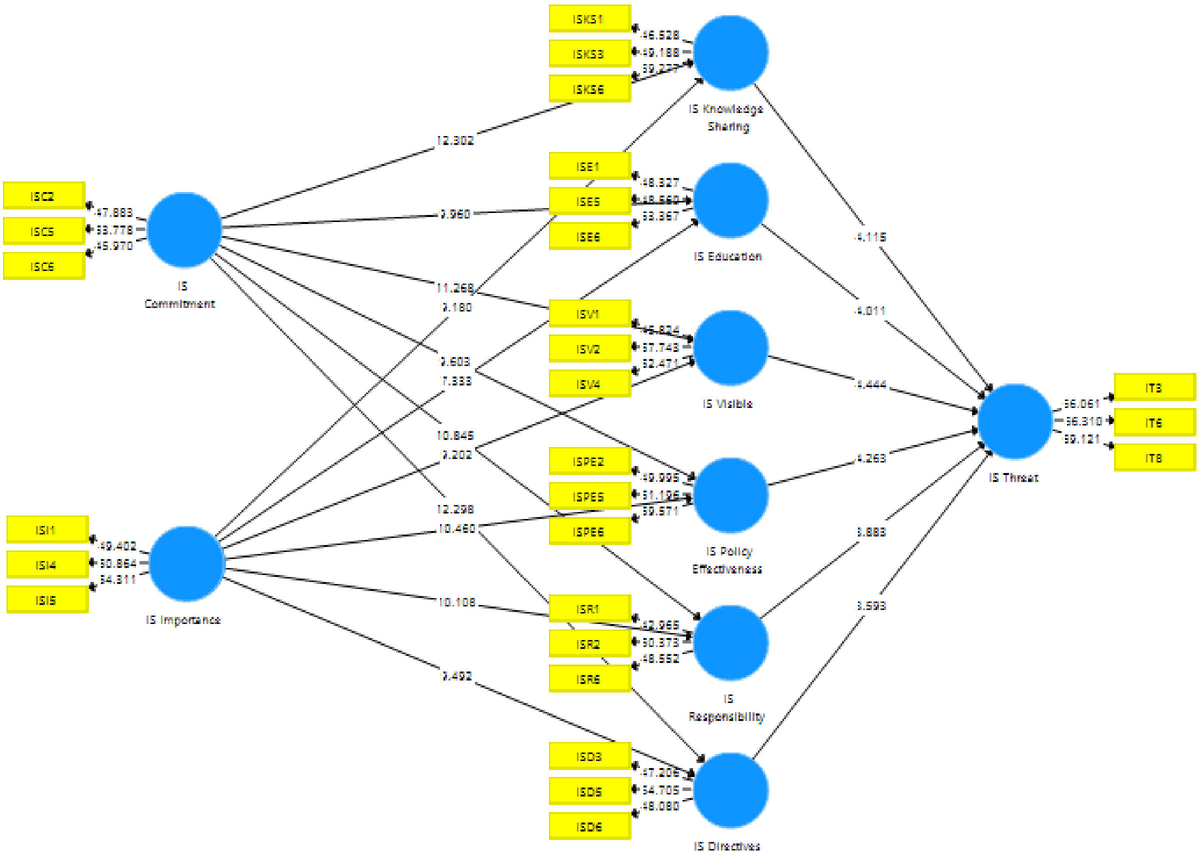

Figure 3: SmartPLS Output of the Structural Model

5. Discussion

This study aims to examine the relationship between the role of top management and organisational ISP and its impact on information security threats. By observing a significant relationship, a positive hypothesis was developed between the top management role construct and organisational ISP, and a negative hypothesis was developed between the organisational information security practical constructs and information security threats. Findings from this study showed that all hypotheses were fully supported. The unequivocal support for these hypotheses suggests that top management's influence on ISPs is both direct and substantive, echoing the assertions of prior studies while providing fresh evidence of the causal significance of managerial actions in organizational security outcomes. Particularly, the study deepens our comprehension of how top management's commitment and prioritization of information security importance foster a security-oriented culture that permeates organizational practices, leading to stronger resilience against information security threats. This study was consistent with the study from Kankanhalli et al. (2003), Kazemi et al. (2012), Alkabani et al. (2014), Humaidi and Balakrishnan (2015), and Masrek et al (2020). In comparison to previous research, this study provides an empirical substantiation on these relationships within the specific context of MD-status organizations, offering a localized perspective on the generalizability of these relationships across different national and regulatory contexts. Moreover, it underscores potential areas for enhancing managerial practices in information security that may have been under-emphasized or overlooked in past models.

As described in the preceding section, the role of top management is operationalised as the combination of ISC and ISI. The synergy between the importance of information security and the commitment of top management can be a driving force to create a safe atmosphere among employees, to be subsequently practiced consciously by every structure in the organisation. This ISP is translated through periodic knowledge sharing and information security education activities among employees.

The organisation's ISP can also reflect the organisation's competence in performing risk assessments against information security threats, further increasing the visibility of the organisation as an organisation that has the ability to deal with information security threats. Organisational ISP that results from the enthusiasm of the organisation's top management for the protection of information security assets also influence the organisation's people to take responsibility for preserving information security assets from facing information security threats either intentionally or unintentionally. The clarity of the information security policy also plays a big role in creating good ISP, and top management has a big role to influence ISP among employees through the provision of information security policies that are clear and can be followed by all employees. Hence, ISP in organisations can be practiced effectively, further reducing the risk of information security threats. The effectiveness of these practices, as revealed by this study's findings, offers substantial contributions to the extant literature, particularly in understanding how the strategic actions of top management permeate through an organization's layers to cultivate a robust culture of security. This study underscores the importance of top management's role not only in policy formulation but also in embodying the values of information security, which in turn can influence employees' attitudes and behaviors, thereby reinforcing the security culture within the organization. Such cultural alignment, bolstered by top management's dedication to ISP, extends the literature by showing how leadership in instrumental in integrating information security into the fabric of daily operations and organizational ethos.

Nieles et al. (2017) noted that "information security is not a static process and requires continuous monitoring and management to protect the confidentiality, integrity, and availability of information as well as to ensure that new vulnerabilities and evolving threats are quickly identified and responded to accordingly". In the presence of top management who is aware of information security can ensure the well-being of confidentiality, integrity, and availability of the organisation's information assets. The findings of this study emphasize the need for such informed leadership and could thus inform the development of future policies that prioritize continuous improvement and dynamic responses to the evolving landscape of information security. Effective policy-making, influenced by top management's active awareness and involvement, could include the establishment of regular training programs, the implementation of advanced threat detection systems, and the fostering of a responsive organizational culture that can adapt to new information security challenges. Moreover, the study's results advocate for the inclusion of information security considerations into the strategic planning at the highest levels of the organization, ensuring that information security management is an integral part of organizational governance and not just a technical or operational concern.

The findings of this study clearly showed that if ISP are implemented effectively in organisations, especially organisations in critical sectors such as IT, health, security, and banking; the risk of information security threats can be reduced, and even if organisations have to face information security threats, they can cope effectively without causing major damage. Since the MD status organisation is a key player in pushing the nation's digital technology developments and the emergence of information security threat patterns that constantly change quickly, it is essential to have an efficient and effective ISP. This is where the great responsibility lies on the top management of the organisation to ensure that ISP can be implemented in the organisation. If the top management is aware of the importance of protecting information assets and gives a total commitment in protecting information assets, the work practices of the organisation can also be indirectly influenced by the attitude of the top management of the organisation towards information security. This proactive stance is crucial in sectors where the protection of information is not just a regulatory requirement but also a cornerstone of customer trust and business continuity. Effectively practices ISPs have the potential to transform the organizational climate into one where a sustainable information security culture is the norm, thus guaranteeing the security of information assets from information security threats. This cultural shift is particularly pivotal in the context of Malaysia's digital economy, where safeguarding digital assets is synonymous with safeguarding the nation's economic future. While the study has underscored the critical role of top management in enhancing ISPs and mitigating threats, it also acknowledges limitations such as the reliance on self-reported data and the potential for response bias. Future research could explore longitudinal studies to examine the evolution of ISPs over time or expand the scope to include a comparative analysis across different national contexts.

6. Conclusion

Two approaches, namely theoretical and managerial, may be used to describe the contribution of the study. Through a theoretical perspective, this study has developed an empirically based framework that connects the role of top management consisting of ISI and ISC with ISP through information security knowledge sharing, information security education, information security visibility, information security policy effectiveness, information security responsibility, and information security directives, as well as connecting the organisational ISP with information security threats. Researchers with an interest in this subject can test the framework in additional contexts in the future. From the practical perspective, this study brings a very clear message to create an effective and conducive information security practice and environment, and it should start from the awareness of the organisation's top management, and then give a high commitment to protect information assets in the organisation.

Despite its contributions, this study was faced with several limitations. First, this study only focused on MD status organisations, the majority of which had a business nature that involved IT. Usually, organisations that have IT as their business nature already have a prior awareness of the importance and threats of information security. Future researchers who are interested should consider doing this study in other settings such as the health sector, finance, security, as well as the government sector. Secondly, this study employed a perceptual measurement device with a cross-sectional temporal horizon for data collection. By its very nature, human vision evolves throughout time. Therefore, future researchers should think about using longitudinal studies to collect data rather than gathering data at a single moment in time since it will help them better understand the correlations between factors.

References

Al-Awadi, M., & Renaud, K. (2007). Success factors in information security implementation in organizations. In Kommers, P. (Eds.), *e-Society 2007: Proceedings of the IADIS International Conference e-Society* (pp. 169-176). Lisbon, Portugal

AlHogail, A., & Mirza, A. (2014). A proposal of an organizational information security culture framework. In Proceedings of the International Conference on Information, Communication Technology and System (ICTS) 2014 (pp. 243-249).

Alkabani, A., Deng., H., & Kam, B. (2014). A conceptual framework of information security in public organizations for e-government development. In Proceedings of *the 25th Australiasian Conference on Information Systems* (pp. 179-189). Auckland, New Zealand

Al-Mhiqani, M. N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K. H., ... & Yunos, Z. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. *Applied Sciences*, *10*(15), 5208.

Bace, R.G. (2000). *Intrusion Detection*. MacMillan Publishing

Chang, S.-E., & Lin, C.-S. (2015). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438-458.

Cohen, J. (1988). *Statistical power analysis for the behavioural science*. Lawrence Erlbaum.

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: a comparison and empirical illustration. *British Journal of Management*, *17*(4), 263-282.

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model information security factors for decision makers. *Computers & Security*, *92*, 1-21.

Ernst & Young (2018). *Is cybersecurity about more than protection? EY Global Information Security Survey 2018-19.* Retrieved from https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf

Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling*. University of Akron Press.

Flores, W., R., 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. https://doi.org/10.1016/j.cose.2014.03.004

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *19*, 39- 50

Geisser, S. (1974). A predictive approach to the random effects model. *Biometrika*, *61*(1), 101-107.

Hsu, C., & Wang, T. (2015). Composition of the top management team and information security breaches. In *Handbook of research on digital crime, cyberspace security, and information assurance* (pp. 116-134). IGI Global.

Humaidi, N., & Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, *5(4)*, 311-318.

Jouini, M., Rabai L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489 – 496.

Kankanhalli, A., Hock-Hai, T., Bernard, C.Y.T. & Kwok-Kee, W. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*,139-54.

Kazemi, M., Khajouei, H. & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. *African Journal of Business Management*, *6* (14), 4982-4989.

Kwon, J., Ulmer, J. R., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. Journal of Information Systems, 27(1), 219-236.

Kudjo, P. K., Wornyo, D. K., & Ocquaye, E. (2017). Importance of information security education and awareness in Ghana. *Communications on Applied Electronics*,*6*(6),30-35.

Liang, H., Xue, Y., & Wu, L. (2017). Ensuring employees' IT compliance: Carrot or stick? Journal of Management Information Systems, 34(2), 1105-1137.

Martins, N., & Da Veiga, A. (2015). An information security culture model validated with structural equation modelling. In Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance. *In HAISA*, (pp. 11-21).

Masrek, M. N., Harun, Q. N., & Sahid, N. Z. (2018). Assessing the information security culture in a government context: the case of developing country. *International Journal of Civil Engineering and Technology*, *9*(8), 96-112.

Masrek, M. N., Harun, Q. N., Ramli, I., & Prasetyo, H. (2019). The role of top management in information security practices [Paper presentation]. *SOCIOINT 2019- 6th International Conference on Education, Social Sciences and Humanities, Istanbul, Turkey*.

Metalidou, E., Marinagi, C. C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. A. (2014). The human factor of information security: unintentional damage perspective. *Procedia -Social and Behavioral Sciences, 147*. 424-428

Masrek, M. N., Soesantari, T., Khan, A., & Dermawan, A. K. (2020). Examining the relationship between information security effectiveness and information security threats. *International Journal of Business and Society*, *21*(3), 1203-1214.

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security. *NIST special publication*, *800*(12), 101.

Noordin, S. A., & Masrek, M. N. (2016, November). Adopting the quantitative and qualitative methods in the social science research: Justifying the underpinning philosophical orientation. In *Proceeding of the 28th International Business & Information Management Association (IBIMA) Conference Seville, Spain, 9-10 November 2016*.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management, 12*(4), 531-44.

Ramayah, T. J. F. H., Cheah, J., Chuah, F., Ting, H., & Memon, M. A. (2018). Partial least squares structural equation modeling (PLS-SEM) using smartPLS 3.0. *An updated guide and practical guide to statistical analysis*, 978-967.

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the royal statistical society: Series B (Methodological)*, *36*(2), 111-133.

Yoo, J. (2014). Comparison of information security controls by leadership of top management. *Journal of Society for e-Business Studies, 19*(1), 63-78.

Zhou, K. Z., Gao, G. Y., Yang, Z., & Zhou, N. (2016). Developing adaptive information security strategies: The critical role of top management support. Journal of Business Research, 69(12), 5552-5560.