INFORMATION SECURITY GOVERNANCE ISSUES IN MALAYSIAN GOVERNMENT SECTOR

RUFIZAH ABDUL MUNIR[1], SHUHAILI TALIB[1*], NURUL NUHA ABDUL MOLOK[1], MOHD RIDZUAN AHMAD[2]

[1]Department of Information Systems, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[2]Department of Software Engineering and Technology, Tunku Abdul Rahman University of Management and Technology, Kuala Lumpur, Malaysia

**Corresponding author: shuhaili@iium.edu.my*

ABSTRACT: Top-level management's commitment and involvement in information security governance are essential in today's interconnected environment. Cyber-attacks are on the rise in this post-pandemic era where organizations rely heavily on the Internet and online transactions. Without proper governance of information security initiatives, information assets could easily be exposed to various cyber threats, compromising the confidentiality, integrity, and availability of organizations' valuable information. Thus, we present four (4) case studies that explore the issues related to the top management of the Malaysian government in information security governance. Drawing on these case studies, we present the real challenges that top management and organizations face when it comes to driving and implementing information security in their respective public sector organizations. We found that top management constraints, resource constraints, challenges in employees' acceptance of information security, and the organization's culture are the major concerns surrounding the security governance and the implementation of information security initiatives in the Malaysian government. Hence, this paper proposed a few solutions to the issues.

KEY WORDS: *Top Management Engagement, Information Security Governance, Security Governance Issues, Information Security Management*

1. INTRODUCTION

The dependency on computers, and Information and Communication Technology (ICT) in running overall business operations, which include technology, people, and process elements, could expose organizations to information security risks (Posthumus & Solms, 2004; Razali & Said, 2015). Many organizations' funding and efforts are directed and focused only on technical components. According to Solms (2006), until the early 1980s, solutions to information security primarily focused on technical issues. However, experts have now realized that technological solutions alone could not guarantee secure mechanisms for organizational information (Safa et al., 2015; Tsohou et al., 2008). Information security issues need to be tackled from a broader, holistic approach to preserving the confidentiality, integrity, and availability (CIA) of information.

Many studies in information security have started to incorporate the human aspects as well as managerial aspects and are no longer limited to technology

issues (Karlsson et al., 2015; Silic & Back, 2014; Siponen & Oinas-Kukkonen, 2007; Soomro et al., 2016; Tsohou et al., 2008). This includes the governance component, where the top management has a vital role in establishing and managing information security in organizations (Soomro et al., 2016; Solms, 2001) to handle business and information technology (IT) risks (Singh et al., 2013). Commitment and managerial roles from the top management are crucial not only to guarantee security initiatives can be implemented throughout the organizations, but also to ensure sustainability and continuous maintenance of information security activities within the organizations.

Empirical research attempts to explore the issues related to top management engagement in information security within public sector organizations are scarce. Given the limited literature on top management engagement's perspective of information systems security, we therefore ask the following research question:

What are the issues faced by the top management in governing information security in their organization?

We begin this paper with a focused review of literature on the challenges revolving around information security governance in organizations. Subsequently, we describe the research methodology, develop a list of information security governance issues in Malaysian public sector organizations and present in-depth discussion on the matter.

2. LITERATURE ON INFORMATION SECURITY GOVERNANCE CHALLENGES

According to the research by AlGhamdi et al. (2020), support for Information Security Governance (ISG) programs continues to face obstacles. One of these challenges involves the support and responsibility of top management for information security. As for the top management, there are still challenges that they must face in addressing issues involving information security governance.

Firstly, top management always sees information security as an operational and technical issue (Molok et al., 2018; Williams, 2001a). The responsibility to manage the protection of information is often relegated to the ICT department or the small security team in the organization. This security team is responsible for ensuring security is being executed properly throughout the entire company, which is impossible without support from the top management. When a security incident happens, top management relies on a technical team supporting an existing technological solution to resolve the problem. Top management is reluctant to invest in more effective information security solutions as it would appear to be a waste of funding (Whitman & Mattord, 2012a). The bigger picture behind every incident is often overlooked. Even though the incident might be minor and does not have much impact on the whole business operations, the root cause and corrective actions need to be properly addressed to avoid more severe impacts in the future.

Secondly, top management may not have sufficient ICT knowledge and expertise to give security direction and IT-related strategies (Jarvenpaa & Ives, 1991; Lankton, 2016). Each organization has security risks, threats and compliance based on the business functions. However, if governance structures and functions are not in place or adequately designed, it is difficult for the employees to exercise

due diligence because security direction is unclear. As a result, it will expose information assets to compromise and reduce their value (Whitman & Mattord, 2012b).

The next issue is that top management does not understand their roles and responsibilities in ISG and Information Technology Governance (ITG) (AlGhamdi et al., 2020; Lankton, 2016), which leads to minimal participation in information security initiatives in their organization (Kim & Kim, 2015). They may be aware of their positions but do not know their accountability, what to do and what to govern. Too few efforts were made to overcome the problem or at least to try to understand it from a strategic level. This result in a much simpler, lazy decision by the top management, leading to the most straightforward solution; subscribing to cyber insurance to mitigate information security issues in their organization (Horne, 2016).

Lastly, an alternative viewpoint from Kim & Kim (2015) about supporting information security is that it is necessary to make suggestions to top management about things that need to be done for continual improvement. No matter what kind of committee it is, like a steering committee, risk management committee, or compliance committee, the top management should be told about the major security agendas. This part of the information security committee's job will help support information security across the whole organization. However, it is hard for top management to join the information security committee, even though they are expected to play a key role (Kim & Kim, 2015; Veiga et al., 2020). IT and security matters are also not included in the agenda of top management meetings (Lankton, 2016). Even if it is discussed in the meeting, the top management only relies on the reports submitted by the operational executives. However, the reports' contents are generic and high-level, without detailed technical and financial information (Bruin & Solms, 2016). Top management also has no time to involve in security as they have many things on their plate (Jarvenpaa & Ives, 1991). Because of this, the top management is not well informed about the organization's efforts in handling the associated risks (Ernst & Young, 2016). Consequently, decisions made in the meeting may not align with the operational team's current issues. This issue is also related to the lack of direction by the top management due to inadequate security knowledge and strategy (Veiga et al., 2020).

These discussions provide an early understanding of top management engagement issues in information security governance. However, there is a scarcity of literature addressing the challenges that top management faces when it comes to governing information security in the government sector.

3. CASE STUDY METHOD, SELECTION AND BACKGROUND

Multiple case study research, especially in the field of information systems research, has previously reported on anywhere from two (2) to six (6) organizations (Eisenhardt, 1989), which influenced our decision to examine four (4) Malaysian public sector organizations. We conducted a multiple case study to examine common patterns of issues focusing on those organizations with different business functions. By studying several ministries and agencies, the research outcome produces robust, powerful data and strengthens the findings.

The organizations were chosen based on the functions they performed in their respective businesses. The similarities and contrasts between these organizations

during the data analysis have been particularly intriguing due to the selections. It agrees with Creswell & Creswell (2018), who state that this form of selection can provide a variety of perspectives on the issues under consideration in the study.

The case study location was initially determined by evaluating a list of ministries. The organizations were then narrowed down to a final list of 12 organizations with various business functions. It was decided that all four (4) organizations would be picked based on their different core businesses to ensure that they were all relevant. Of the four (4) organizations chosen, two (2) are central agencies (CA) (see Table 3.1).

Table 3.1: List of Organizations

Case	***Type of Organization***	***Number of Employees***
Case 1	Development and human resource management (CA)	2,000
Case 2	Telecommunication and broadcasting	704
Case 3	Modernization and reformation of public sectors (CA)	950
Case 4	General administration of public sectors	500

This study employed purposive sampling, as it is the most appropriate technique for studying case studies (Merriam, 2009; Saunders et al., 2016) and because it identifies and chooses individuals who are genuinely knowledgeable and experienced in this study phenomenon (Denzin & Lincoln, 2011; Saunders et al., 2016). We investigated top management/Chief Information Officers (CIOs), information security personnel, and non-information security personnel to gain an understanding of the information security governance issues in Malaysian public sector organizations (see Table 3.2). Interviews served as the primary method of data collection, while participant observations and document reviews served as secondary data sources (Yin, 2017).

Table 3.2: List of Case and Participant

Case	Number of Participants			Total
	CIO/Top Management	Information Security Personnel	Non-Information Security Personnel	
Case 1 (A1)	**1** (A1TM1)	**1** (A1IS1)	**6** (A1NIS1) (A1NIS2) (A1NIS3) (A1NIS4) (A1NIS5) (A1NIS6)	**8**
Case 2 (A2)	**1** (A2TM1)	**4** (A2IS1) (A2IS2) (A2IS3) (A2IS4)	**3** (A2NIS1) (A2NIS2) (A2NIS3)	**8**
Case 3 (A3)	**1** (A3TM1)	**2** (A3IS1) (A3IS2)	**1** (A3NIS1)	**4**
Case 4 (A4)	**1** (A4TM1)	**4** (A4IS1) (A4IS2)	**2** (A4NIS1) (A4NIS2)	**7**

Case	Number of Participants			Total
	CIO/Top Management	Information Security Personnel	Non-Information Security Personnel	
		(A4IS3) (A4IS4)		
			GRAND TOTAL	**27**

There were two phases to the data collection process. A total of five (5) weeks were spent collecting data during the first part of the study. The second phase of data collection, which took approximately four (4) weeks, included follow-up calls and reminder emails given to participants who could not participate in the first interview session due to unforeseen circumstances. In addition, during this second phase, follow-ups were conducted with participants who had previously stated that they would give further information and materials during the first phase of the interviews.

Drawing on the case study results, our analysis showed that although each case study has a different core business, those related to the governance issues are nearly identical for all case studies and show few significant differences. The findings include the constraints faced by top management in handling information security in their organization, constraints in managing financial and labor resources, and constraints in cultivating information security culture, which includes employee acceptance of such culture.

The CIO, who represents the organization's top management overseeing information security activities, has a demanding workload. This is because the CIO has a primary job as a deputy secretary-general for the ministry, depending on the ministry's core business, which often includes policy, administration, and development of the organization. Moreover, the CIO role is an integral part of the position. For example, a deputy secretary-general in charge of administration automatically becomes the ministry's CIO. The majority of CIOs do not have an IT background. Consequently, based on the findings of the interview, nine (9) out of 11 information security personnel believe that the CIO relies heavily on the IT Division, particularly the information security team, when making decisions about information security.

In the public sector, it is typical for organizations to take a reactive strategy to handle issues and incidents involving information security. Nine (9) out of 27 participants concur that attention and action are only given to security incidents after they have occurred. Information security initiatives receive the least amount of attention from the organization's top management since, in their view, information security is more of a support role than a crucial element of the organization's operations. In addition, participants believe that older generations have trouble understanding information security and technology due partly to the generation gap.

In terms of financial constraints, this is something that every public sector organization expects. Top management must exercise caution when spending money and selecting and prioritizing projects that appear to be more critical. Information security efforts must compete for funding with other projects. Even though only four (4) out of 27 participants have mentioned the issue of labor resource restrictions, this constraint must be taken into account by the top

management because of the information security team's burden to drive information security for the entire organization. According to Table 3.7, the number of employees in Case 1 to Case 4 is 500 or more. The size of an organization is determined by the number of employees, according to Corsten (1987). Categorization based on U.S. Small Business Administration (n.d.) as cited by Santoro & Chakrabarti (2002), firms with 500 or fewer employees are considered small, whereas firms with 500 or more employees are considered large. As a result, all case studies are believed to belong to large firms with more than 500 employees. For this reason, top management faces significant hurdles in raising awareness and controlling employees' use of social media to share the organization's confidential information, whether intended or unintentional.

In Case 1 to 4, the organizations already have a culture where the information security audit is more focused on acquiring certification rather than nurturing information security itself. Employees also find it tough to adapt work patterns in order to comply with the information security policy. Perceptions that the task of protecting confidential information is the sole responsibility of the IT Division also become an issue that is difficult to change.

4. INFORMATION SECURITY GOVERNANCE ISSUE

The research question pertains to the issues encountered by top management in effectively managing information security within their respective organizations. This study enables the provision of valuable insights into the concerns pertaining to information security governance within public sector organizations in Malaysia. The attainment of this objective is facilitated by a comprehensive understanding of prior scholarly works pertaining to security governance matters, meticulous analysis of case studies, and constructive discourse on the subject matter.

These issues include the constraints top management faces in handling information security in their organization, constraints in managing financial and labor resources, and constraints in cultivating information security culture, including employee acceptance of such culture, as depicted in Table 4.1.

Table 4.1: Issues in information security governance based on the research findings and the literature review

Issues retrieved from research findings	Issues from the literature review
▪ Top management constraint o Limited bandwidth due to hectic schedule and various meeting agenda o Inadequate knowledge and experience in information security o Reactive in handling information security issues o Information security is not an integral part of the organization's business o Generation gap of top management ▪ Resource constraint o Insufficient budget allocation o Insufficient human capital	▪ Top management always sees information security as an operational and technical issue ▪ The responsibility to manage the protection of information is often relegated to the ICT department or the small security team in the organization. ▪ Top management may not have sufficient ICT knowledge and expertise to give security direction and IT-related strategies ▪ Top management does not understand their roles and responsibilities in ISG and ITG, which leads to minimal participation

Issues retrieved from research findings	Issues from the literature review
▪ Challenges in employee acceptance of information security o Difficult to control staff o Employee lack of information security awareness ▪ Organization's culture o Focus only on passing audit compliance o The misconception of information security and ownership o Difficult to change job routines	in information security initiatives in their organization ▪ Difficult for top management to join the information security committee, even though they are expected to play a key role ▪ IT and security matters are also not included in the agenda of top management meetings ▪ Top management also has no time to involve in security as they have many things on their plate

According to Table 4.1, the study's findings indicate:

- The CIO, who represents the organization's top management overseeing information security activities, has a demanding workload. This is because the CIO has a primary job as a deputy secretary-general for the ministry, depending on the ministry's core business, which often includes policy, administration, and development of the organization. Moreover, the CIO role is an integral part of the position.
- The majority of CIOs do not have an IT background. Thus, the CIO relies heavily on the IT Division, particularly the information security team, when making decisions about information security.
- In the Malaysian public sector, it is typical for organizations to take a reactive strategy to handle issues and incidents involving information security.
- Information security initiatives receive the least attention from the organization's top management since, in their view, information security is more of a support role than a crucial element of the organization's operations.
- Participants believe that older generations of top management have trouble understanding information security and technology due partly to the generation gap.
- In terms of financial constraints, this is something that every public sector organization expects. Top management must exercise caution when spending money and selecting and prioritising projects that appear to be more critical. Information security efforts must compete for funding with other projects.
- Top management faces significant hurdles in raising awareness and controlling employees' use of social media to share the organization's confidential information, whether intentional or unintentional.
- The organizations already have a culture where the information security audit focuses more on acquiring certification than nurturing information security itself.
- Employees also find it tough to adapt work patterns to comply with the information security policy.

- Perceptions that the task of protecting confidential information is the sole responsibility of the IT Division also become an issue that is difficult to change.

5. DISCUSSION

5.1. Top Management Constraint

The schedules of top management are often hectic. Most of the time is taken up by the administration of various things, such as meetings and activities inside and outside the organization. An information security personnel from Case 2 expressed his understanding towards the top management, specifically the CIO, who has many things on his plate. Even though he believes that the CIO could do better in governing information security in the organization, the effort shown by the CIO is sufficient to the fact that the CIO has a lot of things to handle. Consequently, most concerns regarding information security are referred to the information security team to manage.

One of the issues in information security governance is top management's inadequate knowledge and experience in information security and how to ensure that top management has a proper understanding of information security. According to Chang & Ho (2006), top management's IT competence may affect their attitudes toward implementing security standards and willingness to serve in leadership roles within information security management. They may also have more confidence in steering proactive security behaviours. Their comprehension of information security influences the governance patterns they use in information security. However, from this study's findings, it can be seen that top management relies on the information security team to provide input and keep them updated on matters related to information security. Information security personnel from Case 1 to Case 4 have a common view about the knowledge the CIO possesses regarding information security. The vast majority of them are of the opinion that the CIO ought to advance their level of expertise in the area. This is because, most of the time, they communicate with the CIO regarding information security projects within their organization. At the government level, the top management delegates the responsibility for information security issues to the information security team, which results in reduced involvement from the top management in information security concerns. This is contrary to what was stated in the previous literature stated that despite all employees having information security responsibilities, the accountability for managing information security risks and their countermeasures lies on the shoulder of the organization's top management (Fazlida & Said, 2015; Khoo et al., 2010; Williams, 2001b). In order to win over the support of top management, it is imperative that the CIO, who is also a member of top management meetings, constantly discuss the importance of protecting the organization's information assets. It includes highlighting the challenges faced by the IT Division in implementing information security efforts throughout the organization, which require full support and commitment from the top management. Top management needs to be forced to accept the ultimate responsibility to ensure that information security is aligned with the overall business objectives and mission (Budzak, 2016; Solms, 2001; Williams, 2001b).

Based on our observations and analysis findings, we found that a reactive approach was a common and regular practice in Malaysian public sector organizations. In the Malaysian public sector, information security is brought up for discussion and given special attention in the event that a problem or incident arises either inside or outside of the organization. It was disregarded until the incident occurred, at which point it was taken into consideration and action was taken. The reactive approach practiced by the Malaysian public sector is highlighted by a study from Johnston & Hale (2009) which stated that many organizations plan information security reactively, and their asset protection strategies are based on perimeter incidents. One of the reasons for this reactive approach is highlighted by Guo (2013), where in many cases, the function of top management is minimized to that of a supporting role, which is frequently referred to as "top management support". The top management of an organization plays a supporting role, which turns security management into an information technology challenge rather than a business one.

This is in opposition to the concept of ISG proposed by the IT Governance Institute (2006), Solms & Solms (2009) and Warkentin & Johnston (2008), where information security matters need to be integral but transparent in enterprise governance. Putting the information security issues as nothing more than an operational component of IT resulting the top management taking a passive and reactive stance toward security issues, meaning that they try to do something only after security breaches have already occurred. This scenario exists in Malaysian public sector organizations where initiatives pertaining to information security receive the least amount of attention from the top management because of their perspective that information security is more of a support function for the organization rather than an essential component of its operations. As a result of the lack of quantitative information that top management needs to have to optimize security investments, security projects are given less importance (monitoring, budget, etc.) than projects in other disciplines. This scenario supported the literature by Whitman & Mattord (2012), which argues that top management is reluctant to invest in more effective information security solutions as it would appear to be a waste of funding. Top management from Case 3 reported that IT Division needs to make strong justification so that projects under information security could be visible and thus prioritized by the top management. An information security personnel said that security projects are less visible than other projects like system development because everyone uses a system. According to personnel of Case 4, top management is aware of how vital it is to maintain information security; yet, as long as the current implementation does not have any issues, other initiatives that top management considers to be more important are given priority.

Three (3) out of four (4) top management come from the baby boomer generation, with less experience with various forms of technology. When information security concerns are brought up in a meeting, they have difficulty understanding the concept and giving it some thought. Hence, they rely on the IT Division, information security team, or other members of the meeting to support and guide them through the decision-making process. CIO from Case 1, who is also a baby boomer generation, stated that, after reaching a certain level in her career, she becomes complacent and less interested in learning new things, particularly about the technology for information security. Therefore, the information security

governance Malaysian public sector has a greater propensity to stick with the status quo and carry on with the practices that have been established rather than adopting a more proactive and innovative strategy.

It is imperative for top management to recognize and appreciate the significant contributions made by the information security team. The responsibility of the team is to provide education to top management by imparting the most recent advancements in the field of information security. Sustained commitment is required to promote continuous learning and professional development programs among top management, rather than treating it as a singular occurrence. Furthermore, it is advisable for organizations to consider bringing in external experts who can offer valuable perspectives and deliver personalized training that caters to top management responsibilities in information security, while simultaneously harmonizing security initiatives with business objectives. These experts possess the ability to offer impartial viewpoints, offer industry best practices, and help bridge any knowledge gaps.

5.2. Resource Constraint

The lack of adequate financial resources has traditionally posed a significant challenge not only for public sector organizations in Malaysia but also for organizations worldwide. According to research by Gupta & Hammond (2005), the lack of available funds was cited as the primary obstacle faced by 49% of organizations in the United Kingdom when it came to implementing computer security measures. Research on information systems security, on the other hand, indicates that limitations on an organization's financial resources are the second most crucial factor in determining whether or not an organization is ready to implement a technology (Gupta & Hammond, 2005; Karyda et al., 2006; Tejay & Barton, 2013; Wang et al., 2009).

In Malaysian public sector organizations, the amount of yearly funds acquired by each ministry or agency determines how much of the available financial budget will be distributed to them. There are basically two (2) different processes that are used to distribute financial budgets among all of the divisions that make up their various organizations. The first way is through a financial allotment that has been made for each department. The budget is contingent on the planned projects and the results of the projects that came before them. Second, the distribution of financial resources is contingent on the project's significance. This allotment considers the prompt execution of the ad hoc project.

In this study, all CIOs and top management agreed that an inadequate budget is one of the most significant challenges they face when attempting to provide the most effective security solutions for their organizations. Implementing information security projects that involve either increasing the quality of already existing resources or investing in new ones due to cost constraints has been difficult. Because of these constraints, organizations have little choice but to make do with the resources available to them to maintain the security of their information assets, even though they cannot invest in the most cutting-edge security solutions. The top management from Case 3 mentioned that despite the fact that efforts had been made to improve the level of security protection, it could not be implemented due to limitations in the budget. The CIO of Case 3 explained that due to the organization's limited financial resources, they need to try everything in their power to obtain the

budget for the implementation of security measures for their company. This is also due to departments within an organization requiring more immediate attention.

Even though only four (4) out of 27 participants have mentioned the issue of lack of human resources, this constraint must be considered by the top management in the Malaysian public sector because of the information security team's burden to drive information security for the entire organization. Based on this study's findings, the information security team must ensure that all information security initiatives are effectively implemented across the organization. Sometimes, in Case 2, for example, in order to meet the requirements for information security and ICT, members of the team who do not have a background in ICT will need to work together, despite the fact that this is not their area of expertise. However, the issue of human resources is not nearly as pressing as the financial constraints that each Malaysian public sector organization must contend with.

Risk assessments should be carried out by the information security team in collaboration with top management within their organization. Identification of critical assets, potential threats, and vulnerabilities enables organizations to allocate resources based on the level of risk associated with each asset, thereby prioritizing resource allocation. Automation and technology solutions can be utilized by organizations to optimize the utilization of resources. Deploy security tools and technologies to optimize security procedures, minimize manual labor, and augment the efficacy of security personnel. The utilization of limited human resources can be optimized by implementing this approach, thereby enabling the organization to attain higher levels of productivity. Providing employees with the requisite knowledge pertaining to information security can foster an information security culture, without incurring substantial financial costs. The implementation of training and awareness programs for all personnel within the organization can facilitate the attainment of this objective.

5.3. Challenges in Employee Acceptance of Information Security

In the current era of social media, the top management of Malaysian public sector organizations encounters the challenge of disseminating information security awareness to all employees. This is crucial in order to prevent any intentional or unintentional leakage of confidential information on social media platforms.. Top management is responsible for guaranteeing that employees can comprehend the purpose of implementing information security within their organization. This issue is emphasized by Hu et al. (2007), stating that the challenges stemmed from the need to educate employees across all organizational levels and departments on the significance of information systems security in order to ensure that they would be willing to accept the repercussions of their actions when it came to the handling of sensitive data. Top management must ensure that a large number of employees or agencies are in constant compliance with information security standards.

However, according to the study's findings, it is challenging for top management to control hundreds or thousands of employees and ensure they do not leak the organization's confidential information on social media like WhatsApp group chats, as reported by personnel from Case 1. Even if every employee is required to sign the security policy declaration form, the degree to which that person complies with the requirements of the form is something that can be questioned and should be checked. Moreover, support personnel are among those who deal with and have

access to classified papers and information, as stated by personnel from Case 1. Support staff, such as clerks and administrative assistants, who are tasked with protecting a file room containing confidential government files and documents, employment records, and salary information, or a car driver who overhears their boss's conversation while the boss is travelling in their vehicle, are examples of potential risks. Even though officials are frequently the focal point of information awareness efforts and are more exposed to such information security, support staff have a low awareness of information security and are commonly overlooked. We believe that personalized information security education, training, or awareness should be provided to each hierarchical level or division in public sector organizations so that they can relate it to their daily tasks and the nature of their work.

Additionally, based on the findings, there is a problem in which employees do not fully understand the implementation of initiatives relating to information security, like the one mentioned by personnel in Case 2. He stated that after years of implementing the Information Security Management System (ISMS) audit in the organization, members of the organization are still confused with another ISO audit (ISO 9001 Quality Management System) which was introduced earlier in the public sector organizations. This is due to the fact that security audits, such as ISMS, are usually implemented and appreciated by personnel within the certification scope. In Malaysian public sector organizations, the scope of ISMS certification is frequently focused on the data center operating under the IT Division. ISMS implementation is also less prevalent, and as a result, ISMS certification is not popular and well-known within the organization. There is also a common misconception that ISMS is closely connected to ICT and, as a result, falls under the jurisdiction of the IT Division. However, if the ISMS certification gains the attention and support of top management and its scope is expanded to include departments other than the IT division, we believe the audit can be implemented and appreciated by the entire organization.

Everyone contributes in some way, whether directly or indirectly, to the success of the organization's efforts to preserve sensitive information. One of the issues that top management and the information security team have, is ensuring that the entire organization is aware of all initiatives despite having all the documentation in place. Personnel from Case 3 believed there is a need to improve the level of understanding, especially among support staff, regarding the security efforts as they hold so much classified information and documents. There is also the false assumption that information security only applies to departments that deal with ICT or that people do not understand how information security relates to their daily work. This perception needs to shift to make it possible for information security initiatives to be broadly implemented across the entire organization.

Ensuring employee compliance with information security policy can be a challenging task. Customized training programs that align with employees' roles and responsibilities can improve their understanding of the impact of their actions on information security. Training programs that target specific security risks and requirements for different departments or job functions can improve employees' understanding and help them apply the knowledge to their job duties. Creating a culture of transparent communication is essential for promoting ongoing dialogue and encouraging employees to report security incidents or concerns without

hesitation. Encouraging employees to report suspicious activity without fear of retaliation is advisable. Periodic audits and assessments help identify security gaps and vulnerabilities. This practice helps to ensure personnel adherence to established policies and provides an opportunity to correct any misunderstandings or deficiencies in knowledge. Active participation of top management in setting the tone for information security is crucial. They must lead by example and demonstrate unwavering dedication to this critical aspect of organizational operations. It is advisable for top management to follow the same policies, practices, and activities as their subordinates. It is recommended to foster a security-oriented culture within the organization.

5.4. Organization's Culture

For this study, the Malaysian public sector organization's culture is comprised mainly of the perceptions of individuals within the organization – from top management to employees regarding the significance of protecting information assets and the need to maintain an information security culture within the organization. Information security audits enable weighing the level of information security within an organization by evaluating, identifying and rectifying security loopholes. However, information security audits are cumbersome, time-consuming, and performed for certification purposes. Instead of concentrating on inculcating a security culture in the organization, the information security measures that have been established are geared around passing certification audits, as mentioned by one of the personnel in Case 1. In Malaysian public sector organizations, audit implementation only focuses on the scope that falls under the audit's purview and is appreciated by a particular group of personnel within the audit scope, not something that needs to be practiced in the entire organization. Information security audits are also considered burdensome, especially to the implementer, as the top management of Case 3 expressed her regret over the perception.

In addition to the compliance work that needs to be done, according to the observations made by us, an ISMS audit in Malaysian public organizations requires the development, implementation, and ongoing maintenance of a significant amount of documented information. This information includes policies, procedures, and standard operating procedures (SOPs). This security audit appears to be additional work on top of the implementer's regular responsibilities, particularly for the information security team. Furthermore, it is human nature to dislike being questioned, and the audit causes the implementer to feel uneasy because it gives the impression that the auditor is looking for flaws and asking about their work, even though the auditor's job is to help improve the process and help strengthen any information security loopholes that the organization may have overlooked.

Personnel from Case 2 stated that they tried to change the perception of the top management regarding implementing an information security audit. There is a misconception that information security is usually associated with the IT Division since they consider information security as a technical solution. However, preserving information assets requires top management and all employees' responsibilities and making it a culture. This claim is also supported by personnel from Case 4, where people usually relate ISMS with IT Division responsibility. For instance, the top management from Case 3 faces a dilemma in promoting the need for a business continuity plan for every public sector organization due to the

misperception of security requirements. The top management and employees have a preconceived notion of the information security team's function. For example, in the event where the presence of top management is required, they instruct the representative from the information security team to attend on their behalf. The representative must give the top management a detailed description of the event. The rationale is that the information security team has a greater understanding of the work and would be the one to carry it out later. Information security initiatives are complex to realize when management does not appreciate the matter and its relevance, which leads to a bottom-up approach. This finding is comparable to research by Hu et al. (2007) in one of their case studies, where information systems security was always the responsibility of specific personnel in the IT department. Top management, business managers at various levels, and even IT staff who were not directly responsible for security all had the same expectation that security personnel were doing all possible to implement foolproof security technologies and procedures. From the literature and this study's findings, it appears that information security concerns are not among the top priorities of an organization's top management, and changing this image will be difficult.

It is challenging to alter individuals' habits inside an organization to comply with information security policy. They anticipate that the workload will increase in order to ensure compliance with the regulation, resulting in a slow and laborious process. This perception is similar to what Hu et al. (2007) did in their study, where they found that a similar perception underlies the comments of other interviewees who expressed ambivalent or unfavorable attitudes toward security protocols due to their belief that protocols impacted work routines. It becomes a challenge for top management to instill a culture of information security so that employees no longer perceive their work as burdensome. It is difficult to change the routine when the method has been implemented for a long time in the organization. There is a perception that information security is generally the duty of the IT Division and the information security team; thus, obtaining collaboration from other departments to implement information security initiatives throughout the organization is tricky. However, the responsibility for maintaining information security should be split among the various departments that make up an organization, which requires interaction, cooperation, and commitment from employees in all parts of the business Allen & Westby (2007). In order to ensure the continued viability and safety of their organizations, information security issues need to be given the same level of attention as other strategic concerns at the governance level (J. Allen, 2005; Lidster & Rahman, 2018; Whitman & Mattord, 2012b). We believe the process would be more straightforward if there were instructions and support from higher-level management.

Top management's support and active involvement can facilitate the establishment of an influential information security culture. Organizations should communicate the importance of information security to all departments and allocate sufficient resources for its implementation. A comprehensive security awareness program should be implemented, covering all personnel and departments, including those outside of the IT division or information security unit. This enables the alignment of policies and procedures with the organization's specific needs, ensuring comprehensive consideration of all aspects of the organization when implementing security measures. The establishment of cross-functional teams or

committees promotes cooperation among representatives from various departments. Teams can aid in policy formulation and execution, sharing best practices, overcoming challenges, and promoting accountability and shared responsibility for information protection. Optimizing processes and documentation can alleviate security audit burdens. For instance, a centralized repository consisting of standardized templates can simplify the preparation and reporting of audits. Acknowledging individuals and teams who comply with information security policies can serve as a positive reinforcement mechanism, motivating employees to maintain desired behaviors. It is also crucial to communicate information security policies clearly and in a language that all employees can understand, without the use of technical jargon.

6. CONCLUSION

Our case study research explored the issues revolve around information security governance in Malaysian public sector. It provides rich insight from both top management and employees about this pervasive phenomenon, which is affecting organizations globally. The paper also proposed solutions to the issues presented. Information security professionals and policymakers alike can benefit from keeping an eye on this study's findings as they work to strengthen information security programs across the country based on the issues highlighted. Relevant stakeholders, equipped with knowledge of the findings from different points of view, should be able to adapt the proposed solutions in order to improve the present implementation of information security within their organizations.

REFERENCES

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Allen, J. (2005). *Governing for Enterprise Security* (CMU/SEI-2005-TN-023; p. 82). Carnegie Mellon University.

Allen, J. H., & Westby, J. R. (2007). Characteristics of Effective Security Governance. *EDPACS*, *35*(5), 1–17. https://doi.org/10.1080/07366980701394229

Bruin, R. D., & Solms, S. von. (2016). *Cybersecurity Governance: How can we measure it?* 1–9.

Budzak, D. (2016). Information Security—The People Issue. *Business Information Review*, *33*(2), 85–89. https://doi.org/10.1177/0266382116650792

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345–361. https://doi.org/10.1108/02635570610653498

Corsten, H. (1987). Technology transfer from universities to small and medium-sized enterprises—An empirical survey from the standpoint of such enterprises. *Technovation*, *6*(1), 57–68. https://doi.org/10.1016/0166-4972(87)90039-3

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th Edition). SAGE Publications, Inc.

Denzin, N. K., & Lincoln, Y. S. (2011). Introduction: The Discipline and Practices of Qualitative Research. In *The SAGE Handbook of Qualitative Research*. SAGE Publications, Inc.

Eisenhardt, K. M. (1989). *Building Theories from Case Study Research*. *14 (4)*, 532–550. https://doi.org/10.5465/amr.1989.4308385

Ernst & Young. (2016). *Final Report—Global Information Security Survey 2016*. http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016

Fazlida, M. R., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, *28*, 243–248. https://doi.org/10.1016/S2212-5671(15)01106-5

Guo, K. H. (2013). *Revisiting the Human Factor in Organizational Information Security Management*. *6*, 5.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security*, *13*(4), 297–310. https://doi.org/10.1108/09685220510614425

Horne, C. (2016). *Lack of cyber security knowledge leads to lazy decisions from executives*. The Conversation. http://theconversation.com/lack-of-cyber-security-knowledge-leads-to-lazy-decisions-from-executives-68065

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. https://doi.org/10.1016/j.jsis.2007.05.004

IT Governance Institute. (2006). *Information security governance: Guidance for boards of directors and executive management*. IT Governance Institute. http://www.books24x7.com/marc.asp?bookid=30815

Jarvenpaa, S. L., & Ives, B. (1991). Executive Involvement and Participation in the Management of Information Technology. *MIS Quarterly*, 205–227.

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129. https://doi.org/10.1145/1435417.1435446

Karlsson, F., Astrom, J., & Karlsson, M. (2015). Information Security Culture—State-of-the-art Review between 2000 and 2013. *Information and Computer Security*, *23*(3), 246–285. https://doi.org/10.1108/ICS-05-2014-0033

Karyda, M., Mitrou, E., & Quirchmayr, G. (2006). A framework for outsourcing IS/IT security services. *Information Management & Computer Security*, *14*(5), 403–416. https://doi.org/10.1108/09685220610707421

Khoo, B., Harris, P., & Hartman, S. (2010). Information security governance of enterprise information systems: An approach to legislative compliant. *International Journal of Management and Information Systems*, *14*(3), 49.

Kim, K., & Kim, J. (2015). A Role of Information Security Committee based on Competing Values Framework. *Proceedings of the 17th International Conference on Electronic Commerce 2015 - ICEC '15*, 1–4. https://doi.org/10.1145/2781562.2781600

Lankton, N. (2016). *Board Involvement With IT Governance—Practically Speaking Blog*. http://www.isaca.org/Journal/Blog/Lists/Posts/Post.aspx?ID=314

Lidster, W. W., & Rahman, S. S. M. (2018). Obstacles to Implementation of Information Security Governance. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 1826–1831. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00276

Merriam, S. B. (2009). *Qualitative Research: A Guide to Design and Implementation*. Jossey-Bass.

Molok, N. N. A., Ahmad, A., & Chang, S. (2018). A case analysis of securing organizations against information leakage through online social networking. *International Journal of Information Management*, *43*, 351–356. https://doi.org/10.1016/j.ijinfomgt.2018.08.013

Posthumus, S., & Solms, R. von. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638–646. https://doi.org/10.1016/j.cose.2004.10.006

Razali, F. M., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, *28*, 243–248. https://doi.org/10.1016/S2212-5671(15)01106-5

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

Santoro, M. D., & Chakrabarti, A. K. (2002). Firm size and technology centrality in industry–university interactions. *Research Policy*, *31*(7), 1163–1180. https://doi.org/10.1016/S0048-7333(01)00190-1

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students* (Seventh Edition). Pearson Education.

Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security*, *22*(3), 279–308. https://doi.org/10.1108/IMCS-05-2013-0041

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. *Global Journal of Flexible Systems Management*, *14*(4), 225–239. https://doi.org/10.1007/s40171-013-0047-4

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions. *ACM Sigmis Database*, *38*(1), 60–80.

Solms, S. H. (Basie) von, & Solms, R. (2009). *Information Security Governance*. Springer US. http://link.springer.com/10.1007/978-0-387-79984-1

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

Tejay, G. P. S., & Barton, K. A. (2013). *Information System Security Commitment: A Pilot Study of External Influences on Senior Management*. 3028–3037. https://doi.org/10.1109/HICSS.2013.273

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. *Tony & Francis*, 1–30.

U.S. Small Business Administration. (n.d.). *Size standards*. Size Standards. Retrieved 30 May 2022, from https://www.sba.gov/federal-contracting/contracting-guide/size-standards#section-header-0

Veiga, A. da, Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organizational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

von Solms, B. (2001). Corporate Governance and Information Security. *Computers & Security*, *20*(3), 215–218.

von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security*, *25*(3), 165–168. https://doi.org/10.1016/j.cose.2006.03.004

Wang, H., Xu, H., Lu, B., & Shen, Z. (2009). Research on Security Architecture for Defending Insider Threat. *2009 Fifth International Conference on Information Assurance and Security*, 30–33. https://doi.org/10.1109/IAS.2009.53

Warkentin, M., & Johnston, A. C. (2008). IT Governance & Organizational Design for Security Management. In *Information Security—Policy, Processes, and Practices* (pp. 46–68). M. E. Sharpe, Inc.

Whitman, M., & Mattord, H. J. (2012a). Information Security Governance for the Non-Security Business Executive. *Journal of Executive Education*, *11*(1). http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=15351777&AN=85627224&h=Xrrnr%2BcYUwfj9zldJ9IJ7SrqVjgj%2F4Tb%2BWKgGG1ngsYn5RsuWU6QWbHfgtPHQbl87p5DJtZj7E6tJa03hSs3Hg%3D%3D&crl=c

Whitman, M., & Mattord, H. J. (2012b). Information Security Governance for the Non-Security Business Executive. *Journal of Executive Education*, *11*(1), 97–111.

Williams, P. (2001a). Information Security Governance. *IT Governance Institute*, *6*(3), 60–70.

Williams, P. (2001b). Information security governance. *Information Security Technical Report*, *6*(3), 60–70.