ISSN: 2289-4624

EMBEDDING APPROPRIATE SECURITY PRACTICES TO PROTECT ORGANISATIONAL INFORMATION IN TODAY'S CYBERSECURITY LANDSCAPE

Lim Joo Soon [5]

ABSTRACT

There has been widespread recognition that poor information security practices, rather than insufficient technical control, is the primary reason for cyber security attacks. As such, many researchers have called for embedding security practices into organisations to protect organisation's information assets. Despite claims that security practices could prevent organisations from cyber security attacks; there is little empirical work that examines the embedding of appropriate security practices into organisations. This paper argues that organisations should embed the appropriate security practices in a holistic manner to improve the protection of organisational information. The argument is developed through case studies based on semi-structured interviews of respondents, observations, and document analysis from each organisation. The results show that embedding security practices is not as simple as providing security budgets and technical aspects of security. Rather, the more challenging problem is how to embed the appropriate security practices that includes top management support to instil awareness through mandatory training with a clear assignment of responsibility, and enforcement of security policies. The author believes that the findings will provide researchers and practitioners in information security with broader view of the appropriate security practices that need to be embedded to prevent security incidents in today's cyber security landscape.

Keywords: *Malaysia, ketamine, poly-drugs, socio-demographic characteristic, urological problem.*

[5] SAC Dr Lim Joo Soon is currently the Staff Officer of Investigation Unit of SOSMA and POCA at the Royal Malaysia Police Headquarters, Bukit Aman. Email: jslim@rmp.gov.my

INTRODUCTION

Many past researchers and industry practitioners have found that poor information security practices, rather than insufficient technical control, is the primary reason for cyber security attacks. Furthermore, it is widely accepted that information security has moved away from its technical base to a socio-cultural perspective (Dhillon, 2007; Lim, Maynard, Ahmad, & Chang, 2015) and that it has a wide range of other facets which must be considered in order to create a secure information technology (IT) environment (Von Solms, 2001; Wood, 2004).

The information security domain is fairly new and is still an open "playground" (Lim, 2012; Stan, 2007). New trends are being added to this domain as the needs arise with newer and better ways of implementation, depending on the changes and requirements. For example, employees previously thought that information security was a technical issue and that security awareness programs had nothing to do with them. However, as information security has moved away from its technical base, all the employees and departments are responsible for their own information security and all employees must attend awareness programs. As such, when information security is not addressed in a holistic and comprehensive way, taking into account all its dimensions, risks of failing to achieve a secure environment can occur (Lim, 2012; Von Solms, 2005).

In view of that, several researchers and industry practitioners have called for the implementation of appropriate security practices to protect information assets, however they do not elaborate further on what are the appropriate security practices to be embedded in the organisation. For example, Kankanhalli, Teo, Tan, and Wei (2003) contended that the security functions or security practices in an organisation can be classified in various ways. Whereas, Von Solms (2001) postulated that the dynamic nature of information security precludes having fixed boundaries of complete dimensions of information security, and that some of the dimensions may overlap in terms of their content. These findings indicate further research is still needed to understand what are the appropriate security practices to be embedded into an organisation.

Therefore, this paper aims to bridge the gap in literature by examining what the appropriate security practices being implemented to protect the organisation's information assets. In this paper the author argues that research in information security is limited whereby it does not provide details on what are the appropriate security practices implemented in organisations to mitigate or prevent cyber security attacks. This paper explores what appropriate security practices embedded into two organisations are. The paper will review the literature in the area briefly, justify the methods, analyse the results of the case studies, review the contributions and limitations, and conclude by discussing further research directions.

LITERATURE REVIEW

Information Security

The loss of information assets for an organisation can lead to loss of time, money, and more importantly trust in the business world. Thus, it is important to embed security practices to protect organisations' information security. According to the AS/NZS ISO/IEC 17799, information security is

> *"...the protection of information from a wide range of threats in order to ensure business continuity, minimizes business risk, and maximizes return on investments and business opportunities"*
> *(2006, p. vii).*

Effective information security may help both the public and private sectors, for example, telemedicine, distance education, and e-commerce to provide better service and to capture a greater market share. However, in this digital world, organisations become more volatile, changing from conventional large, centralised and hierarchical organisations into broadly scattered informal networks. Consequently, many organisations depend on distributed computing; which includes cloud computing and mobile computing to survive in this dynamic business environment (Rath, 2017).

The development of internet of things (IoT), cloud computing and remote computing has weakened the success of central control. A complicating factor in the rush to cloud computing is organisation's information security. For several reasons, security risks can be intensified by moving it to cloud. As cloud computing grows in popularity, it becomes a popular targets for attackers (Rath, 2017). Although default availability of the "best practices" in security would mark important progress and make deployment and management simpler, Rath

(2017) expressed concern that cloud computing industries still do not fully utilize security opportunities that loud computing offers. Therefore, top management needs to ensure that the appropriate security practices are put in place to protect organisation's information assets (Soomro, Shah, & Ahmed, 2016).

However, many information systems have not been designed to be secured (Lim, 2012). As a result of that, organisations' information systems are faced with security threats from various sources, including fraud, espionage, sabotage, fire and flood. Therefore, in order to remain competitive it is important for top management to ensure appropriate security practices are implemented to protect organisation's information assets.

Information security is multidisciplinary and dynamic in nature (Kankanhalli et al., 2003; Lim, 2012; Soomro et al., 2016; Von Solms, 2001). Thus, information security requires more if not all employees' involvement and participation. Identifying which security controls should be implemented requires proper planning and consideration. Thus, these findings indicates that it is vital for security researchers and organisations to understand what the appropriate security practices are, as it allows taking into account established approaches according to the context that led to their establishment rather than simply taking them for granted. The security practices will be discussed in the next section.

Embedding Information Security Practices

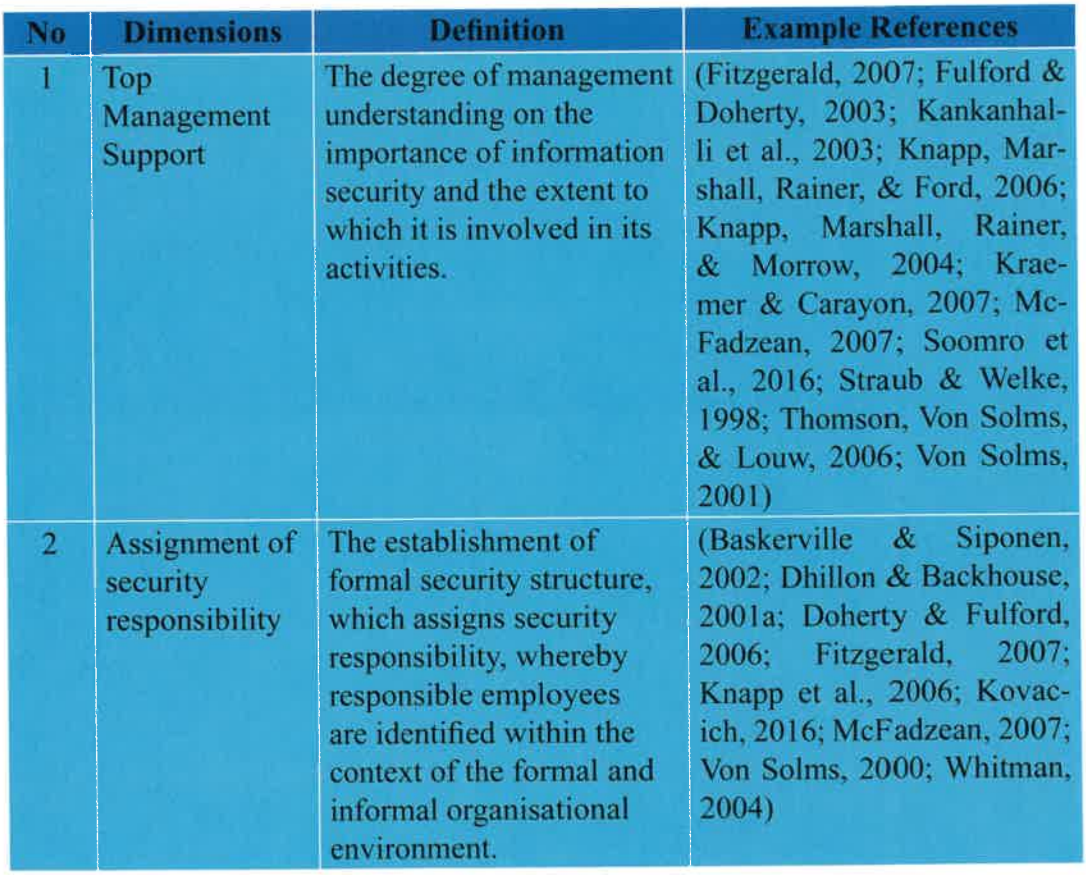
The purpose of this study is to examine what the appropriate security practices implemented in the organisations to mitigate security risks and to prevent cyber security attacks in today's dynamic cyber security landscape. This study uses Lim (2012)'s framework, which was derived from past literature of security practices prior to 2012.

It is evident from the above discussion that security practices are dynamic in nature and multi-disciplinary (Kankanhalli et al., 2003; Lim, 2012; Soomro et al., 2016). Therefore, there is no single ideal solution to manage information security effectively. In addition, security requirements differ from organisation to organisation due to different market environments. Organisations need to understand their security requirements in order to properly implement security practices to survive in this dynamic competitive business world.

In light of the above analysis of literature on security practices, it can be concluded that the prior studies have not extensively investigated security practices and have not comprehensively synthesised the dimensions used. Security practices have been previously studied as though they are adequate and in conjunction with information security management (under confidentiality, integrity, and availability). However, security practices studied thus far have covered only certain aspects of information security rather than providing a comprehensive synthesis, as outlined in Table 1.0.

The framework proposes that top management support is vital in ensuring the appropriate security practices are implemented in organisations. With the participation of top management in security programs, there will be proper assignment of security responsibilities, security policy relevance, security policies enforcement, security training and awareness, security control and monitoring, as well as security communication and reporting mechanism. The following section discusses each of the above mentioned activity.

Table 1.0 Summary of the dimensions of security practices literature



No	Dimensions	Definition	Example References
1	Top Management Support	The degree of management understanding on the importance of information security and the extent to which it is involved in its activities.	(Fitzgerald, 2007; Fulford & Doherty, 2003; Kankanhalli et al., 2003; Knapp, Marshall, Rainer, & Ford, 2006; Knapp, Marshall, Rainer, & Morrow, 2004; Kraemer & Carayon, 2007; McFadzean, 2007; Soomro et al., 2016; Straub & Welke, 1998; Thomson, Von Solms, & Louw, 2006; Von Solms, 2001)
2	Assignment of security responsibility	The establishment of formal security structure, which assigns security responsibility, whereby responsible employees are identified within the context of the formal and informal organisational environment.	(Baskerville & Siponen, 2002; Dhillon & Backhouse, 2001a; Doherty & Fulford, 2006; Fitzgerald, 2007; Knapp et al., 2006; Kovacich, 2016; McFadzean, 2007; Von Solms, 2000; Whitman, 2004)

No	Dimensions	Definition	Example References
3	Security Policy Relevance	The high level of statement of organisation's beliefs, goals and objectives and the general means for their attainment to improve organisation's information security.	(David, 2002; Fulford & Doherty, 2003; Höne & Eloff, 2002; Knapp, Franklin, Marshall, & Byrd, 2009; Knapp et al., 2006; Kraemer & Carayon, 2007; McFadzean, 2007; Straub & Welke, 1998; Thomson et al., 2006; Whitman, 2003 & 2004)
4	Security policy enforcement	The action taken against organisation members who violate security policy to deter others from doing the same.	(Doherty & Fulford, 2006; Fitzgerald, 2007; Fulford & Doherty, 2003; Knapp et al., 2009; McFadzean, 2007; Von Solms, 2000)
5	Security Training and awareness	The training to raise employees' consciousness of the importance of information security. A monitored training and development program required to ensure that processes are performed by competent personnel.	(Doherty & Fulford, 2006; Furnell, 2007; Hentea, Dhillon, & Dhillon, 2006; Knapp et al., 2009; Kraemer & Carayon, 2007; Mitnick, 2003; Pahnila, Siponen, & Mahmood, 2007; Siponen, 2000; Straub & Welke, 1998; Thomson et al., 2006; Von Solms, 2000; Whitman, 2008; Wipawayangkool, 2009)
6	Security communication and reporting mechanisms	Communicating appropriate and inappropriate behaviour to employees so that they understand and believe the importance of security. Also assures individual accountability for any misconduct in relation to security practices.	(Dojkovski, Lichtenstein, & Warren, 2010 ; Knapp et al., 2009; Koskosas & Paul, 2004)

No	Dimensions	Definition	Example References
7	Security control and monitoring	Careful security control and monitoring for a period of time in order to discover non-adherence to security policies and guidelines.	(Knapp et al., 2009; Kraemer & Carayon, 2007; Von Solms, 2000)

Top Management Support

Top management support is essential in implementing information security practices (Lim, 2015; Lim, Ahmad, Chang, & Maynard, 2010; Soomro et al., 2016). They posit that employees will adhere to security policies and procedures if top management shows concern for it. Similarly, Dutta & McCrohan (2002) assert that organisational computer security starts with senior management support and not with firewalls. This is further confirmed by recent research that shows that top management commitment to security is vital in promoting compliant and proactive security conscious users (D'Arcy & Greene, 2009; Soomro et al., 2016). In short, top management must show support by active participation in security programs.

Assignment of Security Responsibilities

Assignment of responsibilities refers to the person or department that is responsible for ensuring the compliance of information security policies (Lim, 2015; Lim et al., 2010). Past researchers and practitioners posit that information security polices need to clearly delineate the responsibilities of everyone in the organisation to protect organisational information (Steve, 2015). If you know that you have sensitive digital information that you do not want stolen, then it is your responsibility to properly secure it. Strawser & Joy (2015) stressed that failure to exercise a reasonable level of due diligence, constitutes a failure on the part of the data-owner. However, past researchers found evidence to suggest that only a small group of people are involved in security activities (Lim, 2012). It suggests that further research is still needed to understand why organisations only assign security responsibility to a small group of people.

Security Policy Relevance

There is a growing consensus both within the academic and practitioner communities that information security policy is the basis for the dissemination and enforcement of sound security practices, within the organisational context (Doherty & Fulford, 2006; Sohrabi Safa, Von Solms & Furnell, 2016). Besides, "it is well known, at least among true security professionals, that formal policy is a prerequisite of security" (David, 2002). Security policy may help organisations develop security awareness by determining appropriate security practices to positively influence employee behaviour to improve organisations' information security (Lim et al., 2010; Thomson et al., 2006). Although past literature agrees that security policy is important in helping organisations to dictate appropriate security practices, yet only a few studies have provided information about the right content of security policy.

Security Policies Enforcement

According to Lim et al., (2010), information security policy may be one of the most important controls to protect organisational information. The main objective of security policy is to influence and direct the actions and behaviours of organisation members (Höne & Eloff, 2002). Security policy also helps to raise security awareness by specifying what is acceptable or unacceptable behaviour in relation to security practices (Sohrabi Safa et al., 2016; Thomson et al., 2006). However, Chia et al., (2002) found that organisational culture support is needed for its development, implementation, and compliance. Their findings show the importance of security awareness in organisations in the context of security policy enforcement towards achieving an optimal level of compliance.

Security Training and Awareness

Security training and awareness programs enable employees to be aware of information security policies and procedures (Bauer & Bernroider, 2017; Öğütçü, Testik, & Chouseinoglou, 2016). Researchers have contended that investing in security awareness training is more useful than investing in security policy (Knapp et al., 2009; Straub & Welke, 1998). The National Security Telecommunications and Information Systems Security Committee (NSTISSC) of the United States require all federal agencies to provide security education, security training and awareness programs for national security systems (Hentea et al., 2006). Despite the importance of security awareness programs in raising employees' security consciousness, researchers often found that employees are careless and fail to comply with security policies and procedures (Pahnila et al., 2007). The author argues that top management has to be convinced and well equipped on the importance of raising employees' awareness.

Security Communication and Reporting Mechanism

Communicating appropriate and inappropriate behaviour to employees through intranet, reminders, periodic briefings, meetings and posters is vital in order for employees to understand and recognise the importance of security and assuring individual accountability for any misconduct in relation to security practices (Lim et al., 2010). Along the same line, Dojkovski et al (2010) argue that the internal marketing of information security is important for communicating information risks, policy and procedure. Furthermore, Albrechtsen (2007) found that poor communication from the information security professionals on how user security behaviour should be, causes users to perform a limited amount of security actions. For Knapp et al. (2009), they contend that enforcement standards need to be formalised, standardised, and written into policies for policy communication and rollout. Therefore, the repercussions and consequences of policy violation are understood by all parties upfront and can be objectively applied in a regulated and fair manner.

Security Control and Monitoring

Security control and monitoring tool can be used as preventive measures to protect against criminal behaviours (Kankanhalli et al., 2003; Straub & Welke, 1998). Organisations increased dependence on information systems requires them to implement sufficient security control to manage the risks associated with those systems (Dhillon & Backhouse, 2001). Similarly, Knapp et al., (2009) argued that organisations need security controls to protect their valuable information in today's high threat cyber environment. Classic examples of security control and monitoring tool in the context of information systems security include: (1) installing security software to obstruct unauthorised access to information systems; and (2) designing physically secure information security facilities (Kankanhalli et al., 2003).

In light of the above analysis of literature on security practices, it can be concluded that many researchers have accepted that information security has moved away from its technical paradigm, and has multiple dimensions that must all be considered in creating a secure organisation. The dimensions of information security discussed above are not necessarily complete, because the dynamic nature of information security prevents any such fixed boundaries (Von Solms, 2001).

METHODOLOGIES

This study aims to gain a better understanding of implementation of appropriate security practices in organisations. As such, the application of case study research to this phenomena is appropriate in a new and emerging area as it is a research strategy that allows for an in-depth exploration in a particular setting (Benbasat, Goldstein, & Mead, 1987; Yin, 1999). Interview protocols were developed based on various issues identified from literature. The author selected two organisations from different industries with expected medium to high level of security risks profile, awareness and knowledge. Participants were selected from top management and employees who are involved in information processing. The organisations demographics are shown in Table 2.

Organisation A is a finance company employing over 5,500 employees providing a diverse range of financial services. The role of the security function in Organisation A is to protect information risks and organisational reputation. Being a financial institution, Organisation A is required by regulations to protect customer information and privacy. In addition, the security functions must also protect organisational reputation to retain competitiveness.

Organisation B is a governmental organisation employing over 96,000 employees providing a range of services. Being a governmental organisation, the role of the security function is to protect the confidentiality, integrity and availability (CIA) of information for top management to make executive decisions.

Financial institution and governmental organisations, both have high risk profiles and need to implement appropriate security practices protecting organisation's information assets.

Table 2: Demographics

	Organisation A (Finance)	Organisation B (Government)
Number of employees	5,500	96,000
Number of Interviewees	8	10
Experience (years)	1-28	4-34
Job Titles	CIO, IT Security Manager, IT Development Manager, HR Manager, Head of Learning and Development, Security and Financial Crime Manager, Business Information Risks Officer (BIRO), Administration Clerk.	Principal Assistant Director of Operation, Assistant Director of IT, IT Security Officer, Assistant Director of Training, Head of Personnel Record, Assistant Registrar of Record, Personnel Record Clerk, Physical Security Officer, Head of Protective Security, Supervisor of Records Department.
Expected Organisation Security Awareness Level	Medium to high	Medium to high

Data was collected from Organisation A (8 participants) and Organisation B (10 participants) via semi structured interviews. The participants are highlighted in Table 2 above. Organisational information security policies and enforcement guidelines were provided for review by Organisation A and Organisation B.

Interviews were recorded and transcribed to transform the collected information with the aim of extracting useful data and facilitate findings. The output of the information was qualitative in nature, therefore the appropriate method by which to accurately identify the correct concepts and themes in the qualitative data collected is through pattern matching (Miles & Huberman, 1994). Pattern codes represents the sets of emergent codes that the researcher develops during data analysis. It helps in reducing the large volume of data into a smaller number of analysis units. Information collected from the documented analysis and observation are also analysed using the same approach.

CASE STUDY RESULTS AND DISCUSSIONS

The goal of this study was to investigate the appropriate security practices implemented by organisations to protect the organisation's information assets. This section includes discussion of top management support in security programs, proper assignment of security responsibilities, security policy relevance, security policies enforcement, security training and awareness, security control and monitoring, as well as security communication and reporting mechanism that uses Lim (2012)'s framework (Section 2.2) to enable the reader to observe the emerging concerns and challenges of implementing appropriate security practices in organisations.

Top Management Support

Organisation A is a finance company that adopts the Business Information Risk Officer (BIRO) structure framework to implement and enforce the information group security policies and group guides. Its top management appointed the Chief Operating Officer (COO) as Chief Information Security Officer (CISO) to demonstrate the seriousness in implementing information security practices. Implementation of information security in Organisation A has always been top down according to the manager of IT development:

> *"Yes, in fact the BIRO structure is headed by CISO, he is one of the top management. So he will assure that this program or whatever initiatives we do will come from the top to the low level. Therefore it has some buy-in and we do have top management support in that sense. CISO is actually the COO of the company".*

Organisation B is a government organisation that has a hierarchical organisational structure. Top management did not appear to understand the importance of the IT division and functions of the information systems. Furthermore, there was no full time Information Technology Security Officer (ITSO) appointed to handle security matters as stated by Assistant Director of IT:

> *"Ideally IT should have its own department. Then we could have a special committee for IT, and then ITSO and CIO are assigned specifically. But what is happening is that the IT division is one of the eight divisions under the Logistics Department and this Logistics Department is among the eight Departments under this organisation. We do not have a full time ITSO and we only appoint officers to perform as ITSO besides their actual role and responsibilities. The answer is we do not have a full time ITSO"*

In addition, there was also less involvement from the management of Organisation B as responded by the Head of Protective Security,

> *"So I am doing my part in my office, respective supervisors must play their role. Imparting the knowledge, sharing information, supervising the personnel under us, but now only 10% of line managers are doing the same thing"*.

Results from Organisation B confirms Fitzgerald (2007)'s cultural view towards information security and Straub, & Welke (1998)'s findings, where information security continues to be ignored by top management and leave the security responsibility to the IT department. In contrast, Organisation A had no problems in getting management support and involvement. Top management involvement is essential in implementing information security practices. Without top management support and involvement, it is difficult to imagine how Organisation B could protect organisation's information assets.

Assignment of Security Responsibilities

The security training and awareness program of Organisation A is managed by the Learning and Development Department. Business Information Risk Officer (BIRO) and Deputy BIRO (DBIRO) across organisation are taking charge of enforcement of security policies. The IT security department was overseeing all

IT security matters. The Security and Financial Crime Manager responded as follows:

> *"When asked who is responsible for conducting awareness program, "For the awareness program we have information security awareness training which is conducted by Learning and Development, our training unit"*

Further evidence of the clear assignment of responsibility came to light when we asked about who is responsible for overall risks. The IT security Manager responded:

> *"As manager of information systems, E-Risk and compliance, it is very specialized section; I look after the compliance of IT whether is from the central bank of from the group. Focusing only IT compliance because we also have the risk department who is in charge of overall risks".*

The security officer of Organisation B focuses more on physical security rather than on information security. In addition, there was no full time ITSO. The training department was more on coordinating courses from other departments and there were no security training nor awareness program ever conducted in Organisation B as explained by Assistant Director of Training:

> *"We are more on coordinate course from various training institutions and departments. If IT division feels that information security is very important, why don't they inform us? Then we will implement. They did not inform us. Security of computer should be from them, I don't have the expertise and I also don't have the knowledge. If they say it is important then we can arrange".*

The findings from Organisation A are in line with the contention of past researchers where a good security policy should clearly assign the responsibilities to various departments and individuals (Whitman, 2004; 2008). Furthermore, a clear assignment of security responsibility may enable employees to better perform and develop their own work practices (Dhillon & Backhouse, 2001b).

In contrast, Organisation B greatly relied on the IT division on security matters. However, they were unable to cope due to heavy workloads. Lack of clear assignment on security responsibilities may jeopardise the protection of organisational information.

Security Policy Relevance

All employees of Organisation A can access the security policy online. The new policy will be published online for employees to access from time to time. The administration clerk replied by giving statement below when asked about the relevancy of security policy:

> *"Yes we read on the intranet. Every information is issued via intranet, ICL, circular. So, if the bank wants to issue new policy, it will be published on intranet on the circular. So we have to be alert at all times, if we want any information, we have to go through the internet".*

As for Organisation B, the security policy was not being updated and many a time, the IT department did not terminate the user id and password of those employees who had left or transferred to another departments as claimed by the Personnel Record's Clerk:

> *We should inform IT (to stop user ID and password in case one is transferred). There is no policy to tell what the process is. We take our initiative to inform. Whoever takes over the duty will be blamed. Because the old staff still has access to the system".*

The results show that Organisation A emphasised on the importance of security policy relevance. They made sure employees can access the security policy. Also any new policies being published should be available to employees via intranet. In contrast, Organisation B did not communicate the availability of security policy to employees. Furthermore, IT did not take prompt action to deactivate employees' user id and password even though they have left the organisation or they have been transferred to other departments.

Information Security Policies Enforcement

As mentioned in Section 4.1, Organisation A adopted group security policies and group guides whereby these policies and guides were enforced by Business Information Risks Officer (BIRO) and DBIRO across organisation as stated by BIRO:

> *"We do have DBIRO, who are checkers that are nominated across the organisation. So they are actually our people in charge in making sure everyone conforms to the clear desk policy".*

Enforcement of security policy in Organisation A is an ongoing activity. When we asked the BIRO how often desks are checked according to the clean desk policy, the BIRO stated:

> *"DBIRO have to perform a clear desk check once a week after office hours report their findings and submit to us every month pertaining to the number of desk checked and breaches found".*

In contrast, Organisation B did not adopt any documented security policies. Instead it adopted orders of logistics department, security orders from security department, and security policies drawn by Malaysian Administrative Modernization and Management Planning Unit (MAMPU) as explained by the Assistant Director of IT:

> *"In actual fact, we do not have security policy in our organisation. We are in the process of developing security policy. However, we are making use of existing guidelines and procedures like Logistic orders, MAMPU's orders and orders from the security office".*

He was very confident that members of the organisation were aware of the security policies as it was advertised via e-broadcast, and the organisation's intranet. However, the Assistant Registrar of Record responded:

> *"I do not know any information about security policies, but I know that we have to login using user id and password".*

The result showed that Organisation A adapted group security policies and guides, and the enforcement of security policies was an ongoing activity. In contrast, Organisation B did not adopt proper documented security policies. David (2002) asserts that policy must be enforced to make it effective. Without the enforcement, "A policy may become a 'paper tiger' with no 'teeth' " (Knapp et al., 2009). The lack of security awareness in Organisation B did not assist enforcement.

Security Training and Awareness

In Organisation A, security training and awareness program is conducted by the Learning and Development Department. Every new employee must go through an induction program within three months of joining the organisation. When asked if security is covered during the induction program, the administration clerk responded:

> *"Under the induction course, we were trained how to protect our information and, not to share information with others even though we are in the same department. I attended both application and security".*

In addition, mandatory security training is regularly arranged for every member including the Chief Executive Officer of the organisation as explained by the administration's clerk:

> *"Annual training is mandatory for all existing staff. Everyone must go through a specific e-learning process. For example, the information risk and compliance".*

In contrast, Organisation B did not have security training and awareness program. The only time employees were exposed to security matters was when they attended application programs as explained by the Assistant Director of IT:

> *"We do not have awareness programs but we touch on security measures whenever there are courses organized by the IT department..... Only then can we incorporate it together with other application programs. This is the time where we create awareness on the security of password, and computer handling".*

However, the Head of Protective Security shared that there was lack of security awareness within Organisation B:

> *"They do not even care about security. From our inspection, the results show that when they go out during break, they never locked the door. All the files are scattered on the desks. Even the classified documents and cupboards are left opened"*

The results showed that security training and awareness program in Organisation A was mandatory and involved everyone in the organisation. In contrast, Organisation B had no security training and only incorporated it in the application programs. Past researchers and practitioners stressed that security training is important to improve security awareness (Wipawayangkool, 2009). Without appropriate security training, it is difficult to raise security awareness of employees in Organisation B.

Security Communication and Reporting Mechanism

Organisation A understands the importance of proper security communication and reporting mechanisms that were put in place to improve the protection of the organisation's information assets. They used the combination of digital and non-digital means to communicate with all employees regarding security initiatives carried out by relevant departments as stated by the Desktop Manager below:

> *"No email to circulate information to all the division heads, section heads, department heads to get any feedback or confirmation if everyone in the group has read the circular. Basically it is to get employees to go through the terms and conditions as well as the desktop parts that we summarised".*

Organisation B are also aware on the importance of security communications and have made efforts to go floor by floor explaining the need to comply with security policies and procedures that were rolled out; as explained by the Human Resource Executive below:

> *"The challenge is the need to constantly remind them that it is important. You cannot take this for granted. You have to follow the steps that had been set and make them understand the implications if they do not follow. We have to get the employees to take it seriously. That is why we have regular awareness briefing floor by floor, and another thing is we have foreign staff and new recruits".*

The results showed that both Organisation A and Organisation B are aware of the importance of security communications and reporting mechanisms in ensuring employees compliance towards security policies and procedures. However, Organization A adopted both digital and non-digital means to communicate with employess regarding security matters. Whereas Organisation B chose to do it by walking floor to floor to explain and remind employees on the importance of complying with security policies and procedures.

Security Control and Monitoring

In terms of security control and monitoring, Organisation A has comprehensive methods in place. Organisation A has both a local auditor and an external auditor to check on the IT systems. Besides that, the IT department also monitors all transactions that are being performed by its staff as elaborated by the Human Resource manager below:

> *"Should I say this is a better control because local auditor can be biased if the local auditor conducts the audit. But instead we are all audited by external auditors. In terms of the systems, we do have what we call an IT security department or section that actually oversees all these IT security in terms of accesses and governance. And all the policies that are derived from there".*

In contrast, Organisation B only imposes a password policy for users to access their information system. It does not have a holistic control nor good monitoring systems as practised by Organisation; as stated by the administration clerk:

> *"Everyone has the password. No clean desk. Only passwords that can be traced back".*

The results show that Organisation A implemented a holistic security control and efficient monitoring method to protect the organisation's information assets. Whereas employees of Organisation B require a password to access their information system. Without appropriate security control and monitoring measures in place, it is difficult to improve the level of protection for organisation's information assets in Organisation B.

In summary, the case studies illustrated the merits of adopting Lim (2012)'s framework to investigate what the implemented security practices are in an organisation. The results showed that Organisation A has strong top managerial support by implementing proper security structure; clear assignment of security responsibilities; periodical security training and awareness programs; ongoing enforcement of security polices and guidelines; proper security control and monitoring systems; as well as security communications and reporting mechanisms put in place to improve information security in protecting organisation's information assets.

The results supported Goodhue & Straub (1991)'s findings that financial firms tend to invest more in security than other firms. First, they relied heavily on information for business operations; secondly, losses from information abuse can be very large; and thirdly, reputation is important to financial firms.

In contrast, Organisation B had less top management support in implementing security practices. It did not have its own documented policies. Moreover, there was no clear assignment of security responsibilities. As a result, the IT division lacked resources in providing a proper awareness program and security training. These results supported (Dzazali, Sulaiman, & Zolait, 2009)'s findings, where only 13% Malaysian Public Service (MPS) were at Level 4 maturity and only 1% were at Level 5 when they evaluated the information security maturity level of information landscape of the MPS organisations. The following section discusses the findings of the case studies and relate the findings to Lim (2012)'s framework.

The following Table 3 summarises how Lim et al. (2012)'s framework might be a useful way of understanding how organisations embed appropriate security practices to protect organisation's information assets. It represents a starting point for examining the embedding of security practices into organisations.

Table 3: The level of appropriate security practices embedded into Organisation A and Organisation B

Appropriate Security Practices	Organisation A	Organisation B
Top Management Support	High level support and involvement	Low level support and involvement
Assignment of Security Responsibility	Responsibilities are clearly assigned	Responsibilities are not clearly assigned
Security Policy Relevance	Periodical updates and reviews. Accessible by all employees	Employees unaware of the existence of security policy
Security Policy Enforcement	BIRO enforcement support	Low enforcement
Security Training and Awareness	Mandatory at all levels	Only mandatory for specific applications
Security Communication and Reporting Mechanisms	Communicated through digital and non-digital means	Relies on traditional face-to-face communication
Security Control and Monitoring	Holistic and comprehensive. Multiple security layers	Dependent only on a password
Maturity of appropriate security practices	High	Low

CONTRIBUTIONS AND LIMITATIONS

This paper offers contributions to the body of knowledge and practice. Given that the majority of current research in this area is conceptual and promotes embedding of appropriate security practices without providing supportive empirical evidence, this paper offer some empirical evidence regarding the embedding of security practices into organisations. For practitioners, the results pinpoint the importance of top management support and active involvement in ensuring the embedding of security practices into organisations. These findings are particularly important as they highlight the main concerns and challenges of embedding security practices into organisations. The results suggests that lack of top management support and involvement in implementing information security practices will affect all security activities in an organisation.

The primary limitation of this paper is that the dimensions of security practices is mainly based on Lim (2012)'s framework. The author believes that additional dimensions like monitoring, control, communication, integrity, and regulatory requirement can be added in future research as Ruighaver et al. (2007) asserted that information security practices are too complex to be covered by a single framework or model. Also, due to sensitivities involved in information security, the author was only able to obtain their information security policy for a short amount of time.

CONCLUSION

Many researchers have called for the embedding of security practices in organisations to improve the protection of organisational information. This paper examines what the implemented security practices are in an organisation. The case study method was used to investigate the two organisations. The results highlighted the main concerns and challenges of embedding security practices into organisations.

The author has illustrated through case studies that the challenges of embedding security practices into organisations are not as simple as investing in information security and the technical aspects of security. The results demonstrates that the implementation of appropriate security practices does not operate in isolation. The roles of top management, assignment of responsibilities, relevance of security policies and enforcement processes, awareness programs and trainings, security communications and control, are appropriate security practices that can make every member in an organisation believe that appropriate security practices are embedded to protect the organisation's information assets. The author believes that the findings have contributed to information security, particularly on appropriate security practices that are embedded into an organisation to protect information assets in today's dynamic and ever challenging cyber security landscape.

REFERENCES

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

AS/NZS. (2006). Information technology — Security techniques — Code of practice for information security management (Vol. ISO/IEC 17799:2006).

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organisations. *Logistics Information Management,* 15(5/6), 337-346.

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organisation. ACM *SIGMIS Database,* 48(3), 44-68.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly,* 11(3), 369-385.

Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2002). Proceedings from the PACIS '02: *Understanding Organisational Security Culture.* Yokohama, Japan.

D'Arcy, J., & Greene, G. (2009). Proceedings from the IFIP TC 8 International Workshop on Information Systems Security Research '09: *The multifaceted nature of security culture and its influence on end user behaviour.* Cape Town, South Africa.

David, J. (2002). Policy enforcement in the workplace. *Computers & Security,* 21(6), 506-513.

Dhillon, G. (2007). Principles of information systems security: text and cases. River Street, Hoboken, NJ: John Wiley & Sons, Inc.

Dhillon, G., & Backhouse, J. (2001a). Current directions in IS security research: towards socio-organisational perspectives. *Information Systems Journal,* 11(2), 127-153.

Dhillon, G., & Backhouse, J. (2001b). Current directions in IS security research: towards socio-organisational perspectives. *Info Systems J,* 11, 127-153.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security,* 25(1), 55-63.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2010). Proceedings from the 21st ACIS '00: *Enabling information security culture: influences and challenges for Australian SMEs.* Brisbane, Australia.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review,* 45(1), 67-87.

Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape and maturity level: case study of Malaysian public service (mps) organisations. *Government Information Quarterly*, 26(4), 584-593.

Fitzgerald, T. (2007). Building management commitment through security councils or critical success factors. In H. F. Tipton (Ed.), I*nformation Security Management Handbook,* (105-121). Hoboken: Auerbach Publications.

Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organisations: an exploratory investigation. *Information & Management & Computer Security,* 11(3), 106-114.

Furnell, S. (2007). IFIP workshop – information security culture. *Computers & Security,* 26(1), 35-35.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of systems users: a study of perceptions of the adequacy of security. *Information & Management,* 20, 12-27.

Hentea, M., Dhillon, S., & Dhillon, M. (2006). Towards changes in information security education. *Information Technology Education,* 5, 221-233.

Höne, K., & Eloff, J. H. P. (2002). What makes an effective information security policy? *Network Security,* 2002(6), 14-16.

Kankanhalli, A., Teo, H. H., Tan, C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management,* 23(2), 139-154.

Knapp, K. J., Franklin, M. R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: an organisational-level process model. *Computers & Security,* 28(7), 493-508.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. *Information and Computer Security, 14*(1), 24-36.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Morrow, D. W. (2004). Proceedings from ISC 2 Survey Results '04: *Top Ranked Information Security Issues.* Alabama: Auburn University.

Koskosas, I. V., & Paul, R. J. (2004). Proceedings from the 6th International Conference on Electronic Commerce '04: *The interrelationship and effect of culture and risk communication in setting internet banking security goals.* New York, NY: USA.

Kovacich, G. L. (2016). The Information Systems Security Officer's Guide (3rd ed.). The cyber security officer's position, duties, and responsibilities (pp. 103-118). Boston: Butterworth-Heinemann.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. *Applied Ergonomics,* 38(2), 143-154.

Lim, J. S. (2012). *Defining the relationship between information security culture and information security practices* (Doctoral dissertation). Retrieved from The University of Melbourne.

Lim, J. S. (2015). Comparative study: the relationship between organisational culture and information security culture. *Journal of Public Security and Safety,* 4(2).

Lim, J. S., Ahmad, A., Chang, S., & Maynard, S. B. (2010). Proceedings from the 14th Pacific Asia Conference on Information Systems '10: *Embedding information security culture - emerging concerns and challenges.* Taipei, Taiwan.

McFadzean, E. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review,* 31(5), 622-658.

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: an expanded sourcebook. Thousand Oaks, USA: Sage Publications.

Mitnick, K. (2003). Best practice: are you the weak link? *Harvard Business Review 81*(4), 18-20.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behaviour and awareness. *Computers & Security*, 56, 83-93.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Proceedings from the 40th Hawaii International Conference on System Sciences '07: *Employees' Behaviour towards IS Security Policy Compliance.* Waikoloa, Hawaii.

Rath, M. (2017). Resource provision and qos support with added security for client side applications in cloud computing. *International Journal of Information Technology,* 1-8.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: extending the end-user perspective. *Computers & Security,* 26(1), 56-62.

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

Siponen, M. (2000). Proceedings from the 15th Annual Working Conference on Information Security '00: Role of human morality in information system security: the problem of descriptivism and non-descriptive foundations. Beijing, China.

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.

Stan, S. (2007). Beyond information security awareness training: it is time to change the culture. In H. F. Tipton (Ed.), *Information Security Management Handbook* (555-565). Hoboken: Auerbach Publications.

Steve, M. D. (2015). Taking responsibility for security. *Computer Fraud & Security,* 2015(12), 15-18.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. MIS Quarterly, 22(4), 441-469.

Strawser, B. J., & Joy, D. J. (2015). Cyber security and user responsibility: surprising normative differences. *Procedia Manufacturing,* 3, 1101-1108.

Thomson, K., Von Solms, R., & Louw, L. (2006). Cultivating an organisational information security culture. *Computer Fraud & Security 2006*(10), 7-11. doi: DOI: 10.1016/S1361-3723(060430-4

Von Solms, B. (2000). Information security – the third wave? *Computers & Security,* 19(7), 615-620.

Von Solms, B. (2001). Information Security – a multidimensional discipline. *Computers & Security,* 20(6), 504-508.

Von Solms, B. (2005). Information security governance – compliance management vs operational management. *Computers & Security,* 24(6), 443-447.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communication of the ACM,* 46(8), 91-95.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management,* 24(1), 43-57.

Whitman, M. E. (2008). Security Policy: from design to maintenance. *Advances in Management Information Systems*, 11, 123-151.

Wipawayangkool, K. (2009). Security awareness and security training: an attitudinal perspective.

Wood, C. C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security,* 2004(1), 16-17.

Yin, R. K. (1999). Enhancing the quality of case studies in *health services research. Health Services Research,* 34(5), 1209-1224.