https://doi.org/10.17576/apjitm-2018-0702(02)-06

http://www.ftsm.ukm.my/apjitm
Asia-Pacific Journal of Information Technology and Multimedia
Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik
Vol. 7 No. 2-2, December 2018: 63 – 77
e-ISSN: 2289-2192

A CONCEPTUAL FRAMEWORK OF IT SECURITY GOVERNANCE AND INTERNAL CONTROLS

NADIANATRA MUSA

ABSTRACT

The Board and senior management use internal controls and IT risk governance to ensure that the corporation's directives such as security policies, standards, procedures, guidelines, administrative rules and practices at all organizational levels are properly chosen and adapted to the organization, implemented and enforced. There were three research problems identified in this paper, lack of involvement of the board and senior management in understanding IS/IT security problems, unbalanced implementation of IS/IT security within the Formal, Technical and Informal components and lack of internal control applications over IS/IT security. This had led to the development of a conceptual framework of IT Security Governance and Internal Controls. Interviews were undertaken with eight Malaysian Publicly Listed Companies to identify the issues that relate to IS/IT Security Governance in Malaysia. The findings reported in the data analysis were consistent with the conceptual framework of IT Security Governance and Internal Controls.

Keywords: IT security governance, internal controls, formal component, informal component, technical component.

INTRODUCTION

In effective corporate governance, boards and senior management direct and control organisational IS/IT assets, resources and data to ensure their business objectives are achieved as intended. They need to ascertain if IS/IT security risks are managed appropriately including those of corporate IS/IT (Institute IT Governance, 2006). In 2006, the IT Governance Institute published a report relating to Information Security Governance, which provides guidance to the Board and Senior Management and IT Security Professionals to assist them in IS/IT Security Governance responsibilities. Many IS Security Professional, Senior Managers and Academics from various industries and many countries such as USA, Britain, Canada, Austria, France, Italy and Australia, were involved in the publication. But, even though internationally recognised, it was rather a guidance and educational resource from a professional body, the IT Governance Institute, than a standard and the report did not include any empirical study for the validation process.

Having IS/IT security controls and security standards in place does not mean that the security of IS/IT is well managed (Baker & Wallace, 2007). As reviewed by Baker and Wallace (2007), previous studies were predominantly focused on the presence or the absence of security controls or security procedures but not on the quality of implementation.

A limitation of standards arises from a compliance-led approach which has influenced the way people implement IS/IT security in organisations. A simplistic, compliance-led approach is not effective for IS/IT security because IS/IT security is not only a technological problem but also a social and organisational problem (Dhillon, & Backhouse, 2000). It has been identified that the three security principles, namely, confidentiality, integrity and availability, were limited and applied to technical perspectives only, they were not applied to organisational

and social aspects. Dhillon and Backhouse (2000) extended the security principles definition to human aspects including responsibility, integrity of people, trust and ethicality.

As IS/IT security involves many disciplinary areas, the board and senior management have to be able to put in place effective mechanisms through IS/IT security controls and IS/IT security standards. An effective mechanism which is internal controls can be used to ensure the placement of IS/IT security controls and standards at any level within the corporation to achieve the corporation's goals. There is a lack of studies that emphasise how IS/IT security controls have been achieved, communicated and reported between and among the board, senior management and all employees.

It has been identified, the research problems in this study are: Lack of involvement of the board and senior management in understanding IS/IT security problems, unbalanced implementation of IS/IT security within the Formal, Technical and Informal components and lack of internal control applications over IS/IT security. These three research problems have driven to the development of two major questions as follows,

Research Question 1: In what way does the involvement of Boards and senior management impact on the implementation of IT/IS security governance?

And Research Question 2: In what way does the directing and monitoring actions in the technical, formal and informal dimensions of IT/IS security governance in corporations be implemented efficiently and effectively?

LITERATURE REVIEW

Internal controls and IT risk governance are essential parts of corporate governance to monitor the effectiveness of resources. To achieve effective corporate governance and minimise business risks, internal controls and IT risk governance are important mechanisms to ensure that resources are used and monitored so that potential security risks can be identified, assessed and mitigated simultaneously.

The Board and senior management are formally responsible for internal controls because they have the power to make decisions on resources and activities, including the security of these resources (OECD, 1999). In other words, IS/IT security is the responsibility of corporate governance and the Board and senior management have oversight of those responsibilities.

IS/IT RISKS AND IT GOVERNANCE

IS/IT assets and resources need to be protected from all risks. Identifying, assessing and mitigating risks are associated with corporate governance. In effective corporate governance, the Board and senior management direct, control and monitor organisational assets and resources including IS/IT to ensure that their business objectives are achieved as intended (Force, 2004). This process is referred to as Information technology (IT) governance, a sub-set of corporate governance.

Within IT governance there are two main responsibilities, IT value governance and IT risk governance. IT value governance concerns the wealth creation of the company and increasing shareholder value while IT risk governance relates to the security of information systems and IT infrastructures. IT risk governance is essential to ensure that organisations derive all expected and intended IT value benefits.

The IT Governance Institute identified five IT governance domains: IT strategic alignment, IT value delivery, IT resource management, IT performance management and IT risk management (IT Governance Institute, (2003). The Institute identified the first four domains as belonging to IT value governance and the last as IT risk governance. When aiming to achieve IS/IT value benefits of the four IT governance domains, safeguarding IS/IT assets and resources is vital to minimise the risks to IS/IT.

Managing the IS/IT risks is an important aspect of IT risk governance. This is for the following two reasons: internal factors and external factors. Internal factors are internal to the

technical dimension and involve risks from technical deficiencies and limitations of the software and hardware. While external factors are concerned with human issues, human threats could be risky to business because many security problems are social and people issues.

Business losses caused by threats to and vulnerabilities of IS/IT may be critical. The literature review has suggested that if threats and vulnerabilities of IS/IT risks are not treated appropriately at the Board and senior management level, security incidents within organisations may continue.

As security of IS/IT is part of IT risk governance, the difference between risk and security needs to be understood first. A risk occurs when a certain system is vulnerable to attacks while security is a process of preserving and safeguarding assets or resources from being attacked. The importance of addressing IT risk governance and ensuring that IS/IT security issues receive a high level of attention has been highlighted by a growing number of security incidents (Lin, 2006).

Risks that result from security threats and vulnerabilities of IS/IT may come from various sources: human threats, e.g., hackers, crackers, computer criminals, terrorism, industrial espionage and insiders; IS application vulnerabilities, e.g., coding problems and physical vulnerabilities, e.g., earthquakes, floods and fire (Dhillon, Tejay, & Weiyin, 2007). That is why the Board and senior management need to be actively involved in corporate risk management to ensure all potential types of IS/IT risks are identified, assessed and mitigated effectively.

IS/IT SECURITY IMPLEMENTATION AND ADEQUATE INTERNAL CONTROLS

A part of the effective management of IS/IT risk includes attention to internal controls. Internal controls are important to the IS/IT security process to ensure the status of IS/IT security is reported so that the board and senior management can react to business risk effectively and efficiently (Solms, 2001). Internal controls are ways, checks and balances, to provide assurance that things go as intended where procedures, regulations and laws are followed, transaction are properly documented, fraud, waste and abuse are minimised, unapproved transactions are not processed and desired outcomes are achieved (Sinclitico, 2007), (OECD, 2002). There are several ways to apply internal controls within IS/IT security implementation such as Model of Corporate Governance Direct Control Cycle by Solms (2006) and the use of General Deterrence Theory by Straub and Welke (1998) and culture factor by Labovitz and Rosansky (1997). The general deterrence theory (GTD) which comes from the field of criminology includes four lines of sequential action, the first is deterrence, the second is prevention, the third is detection and the fourth is remedy, these four lines were developed to reduce computer abuses in corporations (Straub & Welke, 1998).

In the IS/IT security risk planning model by Straub and Welke (1998) which uses GTD, counter-measures work according to lines of controls. In the first line—deterrence control—potential offenders are deterred in a passive approach through policies, guidelines and security awareness programmes. If potential offenders ignore deterrence control, the next line—prevention control—can be enforced actively through physical and procedural controls. If potential offenders successfully penetrate the first two lines, corporations can use detection control to gather evidence of misuse such as suspicious activity reports, systems audits and virus scanning reports. Finally, remedy control is effected when there is non-compliance to the first three lines, which may involve warnings, reprimands, termination of employment and legal action. The four lines of GTD controls are not meaningful if the board and senior management do not put a proper measurement system in place.

However, establishing effective internal controls depends on the involvement of the board and senior management as they are responsible for both the creation of business opportunities and the maintenance of the effective IS/IT security of the corporation (Indrakanti, Varadharajan, & Agarwal, 2007), (Musa & Clift, 2017)

COSO is an example of an internal controls framework but is not exclusively used for guidance in IS/IT security practices and implementation (Swanson, 1999). COSO is primarily used in domains such as financial reporting and audit procedures widely. Organizations used COSO to examine whether certain objectives are achieved as intended by employing certain policies, standards and procedures with senior management's involvement. COSO underlines the role of the board and senior management as the most needed component of a control structure (Bedell, 2006), (Rogers, Marsh, & Enthridge, 2004), (O'Leary, Iselin, & Sharma, 2006).

The Sarbanes-Oxley Act was enacted covering internal controls, external financial disclosure, corporate governance and auditor behaviour (Boyle & Webb, 2007). The enactment of Sarbanes-Oxley Act (2002) was driven by a number of US corporate collapses such as Enron, WorldCom, Waste Management, SunBeam and Global Crossings (Boyle & Webb, 2007). According to Boyle and Webb (2007), in response to the above corporate scandals, the Sarbanes-Oxley Act was enacted covering internal controls, external financial disclosure, corporate governance and auditor behaviour.

Even though the Sarbanes-Oxley Act is not exclusively used for IS/IT, the empirical evidence found that the Sarbanes-Oxley Act is progressively making an impact on the voluntary disclosure of IS/IT activities by corporations (Gordon, Loeb, Lucyshyn, & Sohail, 2006). However, even though the Sarbanes-Oxley Act offers many benefits in US corporations today, there are some drawbacks.

A CONCEPTUAL FRAMEWORK OF IT SECURITY GOVERNANCE AND INTERNAL CONTROLS

Internal controls and IT risk governance are essential parts of corporate governance to monitor the effectiveness of resources. The Board and senior management are formally responsible for internal controls because they have the power to make decisions on resources and activities, including the security of these resources (OECD, 2002). In other words, IS/IT security is the responsibility of corporate governance and the Board and senior management have oversight of those responsibilities.

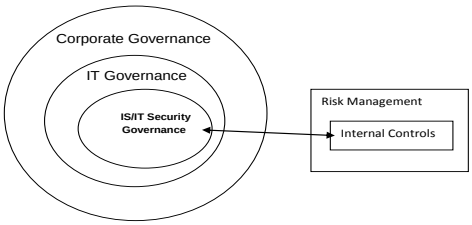

FIGURE 1. Relationship Between Internal Controls, Risk Management and IS/IT Security Governance

As can be seen in In Figure 1, internal controls and IT risk governance work together in addressing potential threats and vulnerabilities at an organisational level. Internal controls are a part of the corporate governance mechanisms.

IS/IT security is a sub-set of corporate governance. It provides strategic direction, achievement of objectives, IT risk governance and the internal controls of the corporate security program. IS/IT security governance in this study is defined as the role of the Board and senior management to establish effective internal controls and apply IT risk governance to ensure that the confidentiality, integrity and availability of IS/IT assets/resources are safeguarded (Baskerville, 1988). Recently, Yassine, Zaydi, Abdelkebir, and Ezzati (2018) developed a practical maturity framework for the Information Security Management and Governance in organizations. The framework has been supported by analysis of data from a survey of 1000

participants with participation rate 83.67% across large and medium companies from various industries.

In this conceptual framework shown in Figure 2, IS/IT potential risks are managed using three dimensions: the technical dimension, formal dimension and informal dimension (Mishra, & Dhillon, 2007).

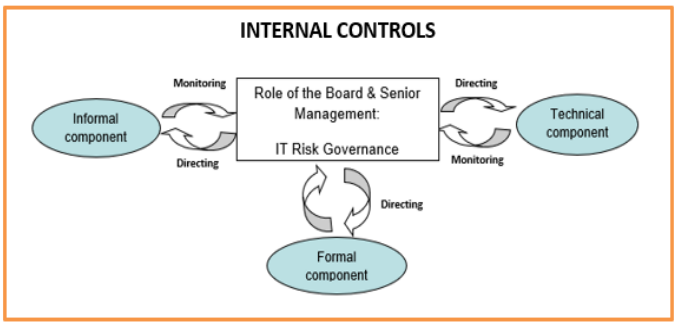

FIGURE 2. A Conceptual Framework Of IT Security Governance And Internal Controls

In Figure 2, the formal dimension is concerned with organisational aspects such as strategic vision and the alignment between business goals and the security policy (Prasad & Green, 2015), (Wu, Straub, & Liang, 2015), (Schlosser, Beimborn, Weitzel, & Wagner, 2015). The security policy includes having clear security roles and responsibilities and other IS/IT security policies. The formal dimension also concerns the organisational structure and formal communications between related roles to achieve the secure operation of IS/IT.

The technical dimension mainly deals with the security of IS/IT areas and uses techniques and controls such as assets classification and control, communication and operations management, access control security (e.g., encryption, cryptography, filters, back up and disaster recovery) and system development and maintenance. The technical dimension is also concerned with how to minimise the vulnerability of systems to coding problems, cloud computing by Rebollo, Mellado, Fernández-Medina, and Mouratidis (2015), Rebollo, Mellado, and Fernández-Medina (2014) and Ula, and Fuadi (2017), big data issues by Moghadam & Ricardo (2018) and also physical threats (e.g., natural disasters).

The informal dimension covers personnel and human aspects such as norms, values, personal beliefs, people's integrity, trust and ethics, culture, commitment, ignorance and stupidity, the level of education and training and security awareness. These aspects facilitate the acceptance of IS/IT security practices within businesses. The informal dimension can be used to address the human threat issues including intended actions associated with hackers, crackers, computer criminals, terrorism, industrial espionage and the inappropriate actions of insiders. The informal dimension includes unintended actions such as mistakes and error.

The three dimensions of IT risk governance need to operate in a parallel way. The Board and senior management are responsible to balance these three dimensions in practice. Ignoring one of these dimensions such as the human aspect may indicate that corporate risk management is not functioning as well as it could be.

Internal controls are important mechanisms to ensure that the alignment between business goals and security initiatives can achieve the corporation's objectives across the formal, technical, and informal dimensions of IT risk governance. Internal controls in the conceptual framework set out in Figure 2 are grouped into two major governance actions, namely, 'directing' and 'monitoring'. The directing actions and monitoring actions can be mapped out across the formal, technical and informal dimensions to achieve an effective implementation of IS/IT security governance (Solms, 2006). As can be seen in Figure 2, directional arrows show that the Board and senior management can provide strategic direction and guidance to the

formal, technical and informal dimensions within organisations. The monitoring arrows indicate how the Board and senior management can monitor the achievement of the actions which were produced in the directed activities. In the monitoring process, all direct activities are monitored to ensure any transactions that occur in the formal, technical and informal dimensions are properly aligned with the security needs as intended.

RESEARCH METHODOLOGY

In this study, qualitative data were collected to answer both research questions. Through the qualitative method, the researcher is part of the research process where the researcher tries to get inside the minds of the directors, senior management and other employees who provide explanations of their situations or behaviours from their own points of view. In the context of IT/IS security governance, the researcher will be able to examine the processes at all levels of activity in the corporation, from top to bottom and from bottom to upper level. Interviews were conducted primarily from the senior managers, junior managers and Board members of Malaysian publicly listed corporations.

Interviews were conducted primarily from the senior managers, junior managers and Board members of Malaysian publicly listed corporations. Using the qualitative method, the researcher aimed to gather two types of secondary data: website data and organisations' documents. The website data like annual reports of Malaysian companies and the organisations' documents like policies relating to IS/IT or IS/IT security were aimed to be gathered in order to strengthen the qualitative results and answer the research questions. To collect qualitative data, the study was conducted multiple interviews using multiple cases. A case is an in-depth analysis which enables comprehensive inquiry and is conducted in the field. Using a qualitative method of data collection like interviews would be expected to increase the trust level and rapport between a researcher and participants. As the area to be investigated is sensitive, a face-to-face interaction may improve the trust level and rapport between interviewer and interviewee(s) and, as a result, richer information on IT/IS security could be gained.

In terms of data analysis technique, content analysis, a traditional technique, was used in analysing the interview data. The columns and rows of a table will be used to organise the data. There will be two major steps involved in this process: first, set up the analysis framework; and second, report results and findings. It was planned in the analysis framework table that all the interview transcripts will be reduced, organised and displayed using themes and sub-themes against issues gained from the interviews. Later, the research questions will be used for arranging the results of analysed data before drawing the conclusions.

RESULTS AND FINDINGS

Interviews were undertaken with eight Malaysian Publicly Listed Companies to identify the issues that relate to IS/IT Security Governance in Malaysia. These include four CEOs who represent the board and management, five CIOs and two other senior managers who represent the senior management team and one junior manager who represents the operational level. In this paper, there were three groups based on the market capitalisation rankings in 2008: Group A, Group B and Group C. From eight companies, three companies came from Group A and another five came from Group B, but none from Group C. The identities of all companies were removed and renamed with a new identifier. The three companies which came from Group A were re-identified as Companies A, C and D, and the five from group B were re-identified as Companies B, E, F, G and H. As for Group A, five participants were involved including one board of director/senior management-CEO, three senior managers with two CIOs and one Business Development Service Director and one junior manager. The CEO of Company A had 20 years experience in the field and 3 years experience as a CEO. All the senior managers of Group A had approximately 10-20 years experience in the field.

In Group B, seven participants were involved in the interview process, three CEOs represented the board/senior management group and senior managers represented by three CIOs and one Chief Financial Officer. The CEO of Company F had 13 years experience as a CEO, one of the most experienced CEOs in this study. The CEO of Company G had worked in the field for 4 years and only 2 years experience as a CEO. The CEO of Company H worked as a CEO for 7 years. While all senior managers in Group B had approximately 10 years experience in their field, except for CIO of Company H who had approximately 2 years experience.

Each company has a different background in industry. The data show that there were six industries: Financial and Insurance, Construction, Plantation, Communication Services, Manufacturing and Mining. The Financial and Insurance industry was represented by two companies from Group B: E and G. The Construction industry had two companies in Group B: B and H. In the Communication Services industry, one company was identified from Group A, C. In the other industries like Mining, one company was identified from Group A which is D. The Manufacturing industry was represented by one company from Group A, A. And one company from Group B, F, represented the Plantation industry.

During data analysis stage, fourteen themes have been identified from the

Formal:

(n=8). (1)

Technical:

(n=3). (2)

and Informal:

(n=3). (3)

components respectively.

THE FORMAL DIMENSION

The formal dimension contains themes that are concerned with the development of formal governance structures of IT/IS security indicating the involvement of boards and senior management in governing IT/IS security. As can be seen in Table 1, the primary issues identified from the interviews were presented into six groups namely business needs, policy development, implementation, monitoring, share role and security issues and budget. From these six primary issues, the interview data analysis has identified eight formal sub-themes comprising Policy, Strategic Vision and Security importance, Compliance/Legal requirements/Regulations, Organizational Structure, Committee, Security Risk and its management and Education/Training/Seminar/Orientation. The instance number shown in table 1 represents the number of interview data found in company A, B, C, D, E, F, G and H.

TABLE 1. Primary Issues and Formal Sub Themes

	Formal Theme 1	Formal Theme 2	Formal Theme 3	Formal Theme 4	Formal Theme 5	Formal Theme 6	Formal Theme 7	Formal Theme 8
Primary Issues	Policy	Strategic vision & security importance	Security internal controls	Compliance/Legal/ Requirem	Organisational Structure	Committee	Security Risk & its Management	Education, training, seminar, orientation

				ents/Regu lation				
Business needs	15	16	15	6			42	24
Policy Development	49					29	4	
Implementation	38	3	17	1	3	2	6	11
Monitoring	11		4		5	2		18
Share roles	1		1		12			
Security issues & Budget		17						

Model of IS/IT security governance – FORMAL Themes (Source from Company A, B, C, D, E, F G and H)

The following presents evidences that found from three primary issues; business needs, policy development and security issues and budget.

BUSINESS NEEDS

SECURITY VISION AND SECURITY IMPORTANCE

IT/IS security is important in order to achieve the maximum use of IT/IS for wealth benefits and cost cuts in business. As one CEO noted and identified in the formal dimension and the technical dimension:

"CEO F: Our corporation is highly dependent on IT and most of our systems are electronically digitally set up, I mean we have IT on our Finance Integration of Financial Statement Information Accounting, we have Integrated Financial System which is linked very closely with our Plantation Management System and also linked directly to our Human Resource Information Systems (HRIS). So among the three of these, software and the systems we have used for accounting systems will be used directly for reporting in our corporation. We have Management Information Systems (MIS), reporting on critical issues and using all this stuff, so security of IT/IS it is very important to us".

Security Risk and its management

Three CEOs and three CIOS had reported IT/IS security risks were part of their business risks management plan. As with other risks, security risks issues need to be identified and mitigated effectively and efficiently to increase shareholder value and profits. As one CEO noted in the following response: *"CEO A: Company A Malaysia believes that effective management of risks associated with all aspects of the organisation's business is critical for sustained growth and continued enhancement of shareholder value. Like many other matters, IT-related matters are also constantly reviewed as part of the organisation's Enterprise Risk Management programme."*

Security Internal Controls

Good internal controls rely on the tone of the board and senior management and ensure that the investment of resources is correctly used to achieve its goals. The CEO of one corporation confirmed the vital role of the board and senior management to control the environment successfully, identified in the formal theme:

"CEO A: Yes, Company A Malaysia has a system of internal control which includes the establishment of an appropriate control environment and framework. The Board of Directors are the owner of the system of internal control as they establish the tone at the top of the organisation, ensuring that the importance of internal control is understood and that the correct resources are available".

In the corporation's structure, the participants worked closely with committees like Audit and Risk to ensure that the internal controls of IT/IS security policies and procedures were complied with which is described in the following quotation.

"CEO F: we are actually very concerned about the risk managing part and our auditors and external auditors actually look to our IT/IS security and comment on whether we have enough controls and also when we have back up".

POLICY DEVELOPMENT

POLICY

Participants were involved in the formulation and implementation of policy relating to IT/IS security. IT/IS security policy, like all other policies, is approved by the Board and senior management. Many comments supported these notions associated with IT/IS security policy in place.

The CEO of Company F stated :

"The management headed by myself, and of course the IT department and the internal audit were involved in the formulation of IT/IS security policy. We have a number of policies and procedures here, you may want to have a look the major headline of policies relating to IT/IS security- System information access control, Physical and environmental security, Network management, Back up and restoration, System back up and ownership, IT system change management, Problem management and IT system capacity management."

There are other examples of involvement in IT/IS security policies.

The CEO of Company A highlighted the security issues areas of policy covered in his corporation:

"The security issues that are included here in the policy are related to network connectivity, account management, vulnerability management, secure system development, incident management, host protection and authentication".

The CIO of Company B reported:

"We have five basic security policies that cover backup, internet use, email use, desktop appearance and data classification."

The CIO of Company D shows what his security policy covers, including mobile:

"For security areas, it covers everything, e-mail policy, information security, I mean in terms of what kind of information you can disseminate, in terms of you labelling the information, confidential, secret, internal use, and then desktop management inclusive, network, mobile. Mobile is formed under baseline, because security, inside a lot of items there, a lot of things, desktop baseline, quite several of baselines, very extensive in terms of (the area covers). We have also internet policy. In which it mentioned, all the internet facilities are meant for company purposes. In fact some of the non-business related sites are being blocked for staff to access."

As noted by the CEO of Company G:

"the security policy covers issues like access, return to operation (system down) and acceptable run time."

Security risk and its management

The identification of security issues was a part of the risk management process. Different corporations have different organisational structures for identifying and managing their security risks as described in the following.

"These security issues are identified mainly by the IT staff with assistance from Business Security staff in Company A Malaysia. They ensured that the decisions were appropriate to the business risks, measured against industry best practices and sat within Company A Malaysia's existing governance and policy structures wherever possible". (CEO, Company A)

SECURITY ISSUES AND BUDGET

COMMITTEE

Security issues can be identified at any committee as described below.

"We do have IT steering committee. We have four committees that look overall issues- Divisional Management Committee (overall issues), Division Planning Committee (specific

issues), Operation Technical Committee (OTC) (operation issues) and Divisional Risk Committee. So if we have IT or security issues, we discuss with Division Planning Committee. The security issues are identified through the Divisional Officer during the Council Meeting, at the forum and through committee." (CIO, Company C)

In the case of Company D, the decision process on security issues is partly shared with its parent company structure called "Corporate IT Development Unit".

"In directly since the policy and procedures was crafted at Corporate IT Development Unit level so in a way we have to be liaising a lot with Corporate IT Development Unit, getting some directions, some inputs, some recommendation, of course we make some decisions as well, of course when come to certain issues, if we think it warrant to be brought up to Corporate IT Development Unit we will, same goes to any security issues, we think if we can manage at our own level with I-Pgroup, we will do that". (CIO, Company D)

As IT/IS security governance is the responsibility of the Board of directors and senior management, the security issues brought up to the senior management level can be seen in the following comments by the CEO of Company A.

"These issues are identified through the organisation's Enterprise Risk Management process whereby the Risk Management Team headed by the Finance Director and comprising senior managers from all departments in the organisation including IT, will conduct quarterly reviews of the business risks as part of their responsibilities".(CEO, Company A)

The interviewees revealed that security issues involve human aspects, technical, lack of policy implementation and natural disasters. The following evidence of security issues was found. The CEO of Company H said:

"Security issues include virus attack, hacking, sabotage, poor access control, lack of proper backup facilities, inadequate or outdated hardware or software and natural disasters."

In the case of Company B, virus is also part of security issues. While network management was considered as a major security issue by Company C.

In some cases, participants reported that security issues were part of the IT/IS budget. This may indicate that some of the Boards of directors and senior management really are involved in the implementation of IT/IS security governance. As the CIO of Company H reports:

"Mainly security issues included within the budget include IT training, routine expenses to maintain IT security like anti- virus, anti-spam control, firewall and updates".

The CIO of Company E commented:

"Security issues included within the budget-unauthorised access, disclosure, modification, destruction and theft".

And the CIO of Company D noted on security issues and budget:

"..internet and antivirus are also part of the security issues included in the budget, we do have agreement with the service provider, every now and then antivirus is updated and distributed across. And this is being budgeted on yearly basis."

The technical dimension contains themes that reflect security controls development and implementation and the responsibility of boards and senior management. Boards and senior management are accountable for the success or failure of planning, development, implementation and maintenance of security controls. Three technical sub themes were identified, "techniques and controls", "system development" and "internet or network security", see Table 2.

TABLE 2. Primary Issues and Technical Sub Themes

Primary Issues	Technical Theme 1	Technical Theme 2	Technical Theme 3
	Technique & Controls	System Development	Internet/Network Security
Business needs	10		1
Policy Development Implementation	14	1	11

Monitoring Share roles			
Security issues & Budget	18	1	15

Model of IS/IT Security Governance – TECHNICAL Themes (Source from Company A, B, C, D, E,F,G and H

The following presents the interview data from sub Technical theme namely technique and controls:

Security control was identified as an important technique to achieve IT/IS security. Business information should not be altered or modified by irresponsible people. For example, one response stated, *"CEO F: We take great care to safeguard our system adopting firewalls and security systems like "Tom Access" where at certain levels we use passwords to enter the systems."*

Security internal controls can be divided into four types, deterrence, preventive, detective and remedy controls. Deterrent applies a passive approach likes policy and security awareness. Preventive uses an active approach such as password controls. If the preventive control has been ignored, the detective countermeasures will take place such as security reports or virus reports. The remedy control can be used if all of these three controls fail such as termination and warnings. One company used preventive and detective controls as part of achieving security internal controls,

"internal controls we would have preventive and detective controls and our audit department regularly review whether internal controls are in place whether there is any breach of the IT policy procedures security, whether any breaches in terms of the IT, and always check and balances". (Chief Financial Planner, Company F),

IS/IT security internal controls may vary. One participant mentioned the security internal controls used in his organisation were hardware control and password control. Both types of control were considered as preventive controls to mitigate the security risks,

"To monitor the policy and procedures, we have security controls in place to identify breach of policy, let say the internet policy. Internal controls are in place to alert us to security breaches. We also have a hardware appliance that allows us to block access to websites we do not wish staff to access. Our controls are mainly related to intrusions – the machine shuts down on a third attempt to intrude. We have in place a password security system and user verification process" (CIO, Company B).

Similarly, the use of password counter-measures for security internal controls were used in another corporation.

"Safeguarding sensitive information is our risk management plan to ensure our IS/IT information such as Balance Sheet, Accounting and Reporting System, MIS, Accountable Budget, other Accounts, Future Profit of Company and Forecasting Information of Market Share Price are not stolen by hackers and disgruntled employees. That is why password protection is part of our internal controls. If this is not addressed, our sensitive information might be published by irresponsible people and ultimately damaging our corporation's name due to weak security systems" (CEO, Company F).

The informal dimension reflects themes embracing human aspects in regard to levels of knowledge and skills, awareness, level of human integrity in IT/IS security implementation. Integrity refers to levels of honesty by staff as seen in Table 3.

Three sub themes were identified: "staff integrity/ethicality/accountability", "culture/commitment" and "human issues-lack of awareness/stupidity".

TABLE 3. Primary Issues and Informal Sub Themes

Primary Issues	Informal Theme 1	Informal Theme 2	Informal Theme 3

	Technique & Controls	System Development	Internet/Network Security
Business needs	12	2	5
Policy Development			
Implementation	2	2	3
Monitoring	1	1	1
Share roles			
Security issues & Budget			

Model of IS/IT Security Governance – TECHNICAL Themes (Source from Company A, B, C, D, E,F,G and H

The following addresses the interview data from sub Informal theme namely culture and commitment,

"*CEO A: Informal factors are very important to support the implementation of IT security policy and controls. Successful IT security policy and controls is not just the deployment of technology (firewalls and intrusion detection systems) but is a series of essential practices that is embedded into the culture of Company A Malaysia through training, education, awareness and others".*

Employee Values refer to people's integrity, trust or ethicality, which deal with personnel values of employees. Integrity of people is part of the organisation. For example, as noted by the CEO of Company G,

"I think the core values, such as integrity are fundamental and everything".

In addition, Employee Values should not be included in the policy statements because they are part of the requirements of membership of an organisation,

"Core values such as integrity, accountability and trust are not subject to policy statements. They underlie or are at the foundation of the business. For example, the way we interact with each other and the way we engage between internal users and customers (Company G)".

A similar view by CEO of Company F, Employee Values are the basis for business and part of security culture and beliefs,

"Culture and company and all that, they know that our own ethics, knows our culture and company, and our expectation that must be, integrity must not be questionable, once we know we trust them, we must be able to empower them".

According to the CEO of Company H, moral value plays an important role towards successful IS/IT security implementation,

"Informal factors will affect the human aspects like morale hence their support in the implementation of policies and security controls (CEO, Company H)".

Lack of people's integrity and lack of accountability may threaten the IS/IT system processes because security is not only a technical problem but also a social problem.

"Informal factors are important to support the implementation of IS/IT security because if people are not accountable and lack of integrity, the system processes would be compromised (CEO, Company G)".

In addition, security culture should be cultivated within the corporate agenda as addressed by CEO Company G,*"CEO G: Imbue a culture that is aligned with the Board approved corporate strategy, mission, values, objectives, policies and procedures; and fosters risk awareness culture"*

DISCUSSION AND CONCLUSION

Generally, the findings reported in the data analysis were consistent with the conceptual framework of IT security governance and internal controls. Fundamentally, the study has answered the two research questions posed through findings reported in previous section. In

answering Research Question 1, "In what way does the involvement of Boards and senior management impact on the implementation of IT/IS security governance?", multiple cases analysis was conducted using manual content analysis and found evidence about the development of IS/IT security aspects with regard to the formal, technical and informal components; these findings have reinforced the themes developed in the model of IS/IT security governance. Fundamentally, all the issues identified in the interview data supported the three dimension themes, formal, technical and informal . Most of the results of interview data analysis supported the elements of formal themes, which included IS/IT security vision, IS/IT security management strategy and IS/IT security policy. Some results of the interview data analysis supported the elements of the technical themes of the model, comprising technological resources and IS/IT security procedures. While the elements of the informal themes including employee values, organisational values and culture, norms and beliefs, were supported by some results of the interview data. To answer Research Question 2, "In what way does the directing and monitoring actions in the technical, formal and informal dimensions of IT/IS security governance in corporations be implemented efficiently and effectively?", single case analysis was conducted. The single (company) case analysis supported the directing and monitoring action over the three components and component interactions. The content analysis supported the interaction of a component (formal or technical or informal) with another two components (formal or technical or informal) with regard to the directing and monitoring actions in three types of interaction: 1) the Formal component and its interaction, 2) the Technical component and its interaction and 3) the Informal component and its interaction. The majority of findings supporting the model of IS/IT security governance was provided by big industry players among Malaysian Publicly Listed Companies.

ACKNOWLEDGMENT

Faculty of Computer Science and Information Technology, UNIMAS and University of Tasmania, Australia, Bursa Malaysia.

REFERENCES

Baker, W., & Wallace, L. 2007. Is Information Security Under Control?: Investigating Quality in Information Security Management. IEEE Security And Privacy Magazine, 5(1), 36-44.

Baskerville, R. 1988. Designing Information Systems Security. New York: John Wiley.

Bedell, D. 2006. Security Complex. Global Finance, 20(6): 25.

Boyle, G. & Webb, E. G. 2007. Sarbanes-Oxley and its Aftermath: A Review of the Evidence. https://ir.canterbury.ac.nz/bitstream/handle/10092/2438/12614152_Sarbanes-Oxley01b.pdf?sequence=1&isAllowed=y [23 December 2018].

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

Dhillon, G., & Backhouse, J. 2000. Technical opinion: Information system security management in the new millennium. Communications Of The ACM, 43(7), 125-128.

Dhillon, G., Tejay, G., & Weiyin, H. 2007. Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations. https://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550157b.pdf [22 December 2018]

Force, N. C. S. S. T. 2004. Information Security Governance: A Call to Action. http://www.isacaroma.it/pdf/news/0412-gbsecgovernance.pdf [30 December 2005].

G. Labovitz, & V. Rosansky. 1997. The Power of Alignment: How Great Companies Stay Centered and Accomplish Extraordinary Things. New York: John Wiley & Sons, Inc.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. 2006. The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities. Journal of Accounting and Public Policy, 25(5):1-41.

Indrakanti S., Varadharajan V., & Agarwal R. 2007. On the design, implementation and application of an authorization architecture for web services. Int. J. Information and Computer Security, 1(2):64-108.

IT Governance Institute. 2003. Board briefing on IT governance. Rolling Meadows: IT Governance Institute.

IT Governance Institute. 2006. Information Security Governance: Guidance for Boards of Directors and Executive Management ; 2nd Edition. Rolling Meadows. ISACA.

Lin, P. P. 2006. Systems security threats and controls. https://washburn.edu/faculty/espahbod/A625_files/System-security-threats-and-controls.pdf [20 December 2018].

Mishra, S. & Dhillon, G. 2007. Information Systems Security Governance Research: A Behavioral Perspective. https://pdfs.semanticscholar.org/3f74/9f754d05d7a46a2e4f39fd019c1d00b54323.pdf [23 December 2018].

Moghadam, R. S., & Ricardo C. P. 2018. Information security governance in big data environments: A systematic mapping. Procedia computer science 138: 401-408.

N. Musa, & B Clift. 2017. Internal Control and Standard Operating Procedures in Malaysian Corporations. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(2-10):25-31.

OECD. 1999. Principles of Corporate Governance. Paris Cedex. OECD.

OECD. 2002. OECD Guidelines for the Security of Information Systems and Networks: Towards a culture of security. https://www.oecd.org/internet/ieconomy/15582260.pdf [23 December 2018].

O'Leary, C., Iselin, E., & Sharma, D. 2006. The Relative Effects of Elements of Internal Control on Auditors' Evaluations of Internal Control. Pacific Accounting Review: Accounting & Tax Periodicals, 18(2): 69.

Prasad, A. & Green, P. 2015. Governing cloud computing services: Reconsideration of IT governance structures. International Journal of Accounting Information Systems, 19:45-58.

Rebollo, O., Mellado, D., and Fernandez-Medina, E. 2014. Isgcloud: a security governance framework for cloud computing. The Computer Journal, 58(10): 2233-2254.

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. 2015. Empirical evaluation of a cloud computing information security governance framework. Information and Software Technology, 58: 44-57.

Rogers, V. C., Marsh T. A., & Enthridge J.R. 2004. Internal Controls: Winning the battle against risks. Internal Auditing ABI/INFORM Global, 19(4): 28.

Schlosser, F., Beimborn, D., Weitzel, T., & Wagner, H. T. 2015. Achieving social alignment between business and IT–an empirical evaluation of the efficacy of IT governance mechanisms. Journal of Information Technology, 30(2): 119-135.

Sinclitico, G. 2007. Management Controls Have Finally Gone Away!. https://ignet.gov/sites/default/files/files/sp07jpi.pdf [23 December 2018].

Solms, B. V. 2001. Corporate Governance and Information Security. Computers & Security, 20(3): 215-218.

Solms, B.V. 2006. Information Security- The Fourth Wave. Computers & Security, 25 (3): 165-168.

Swanson, R. M. 1999. Internal Controls: Tools, not hoops. Strategic Finance, 81(3):6.

Ula, M., & W. Fuadi. 2017. A Method for Evaluating Information Security Governance (ISG) Components in Banking Environment. Journal of Physics: Conference Series. 812(1): 1-7.

Wu, S. P. J., Straub, D. W., & Liang, T. P. 2015. How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. Mis Quarterly, 39(2), 497-518.

Yassine, M., Zaydi, M., Abdelkebir, S., & Ezzati, A. 2018. Building a Maturity Framework for Information Security Governance Through An Empirical Study In Organizations.

https://www.researchgate.net/publication/325555260_Building_a_maturity_framework_for_information_security_governance_through_an_empirical_study_in_organizations [23 December 2018].

Nadianatra Musa
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak (UNIMAS)
Kota Samarahan, Malaysia
nadia@unimas.my

Received: 28 June 2018
Accepted: 31 August 2018
Published: 17 January 2019