A Conceptual Framework of IT Security Governance and Internal Controls

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

***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, (1) Lack of involvement of the board and senior management in understanding IS/IT security problems, (2) unbalanced implementation of IS/IT security within the Formal, Technical and Informal components and (3) 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

I. 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 [1]. 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/IT is well managed [2]. As reviewed by [2], 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 [3]. 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. [3] extended the security principles definition to human aspects including responsibility, integrity of people, trust and ethicality.

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?

II. LITERATURE REVIEW

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 [4]. In other words, IS/IT security is the responsibility of corporate governance and the Board and senior management have oversight of those responsibilities.

A. 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 [5]. 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.

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.

978-1-5386-7541-0/18/$31.00 ©2018 IEEE

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 [7].

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 [8].

B. *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 [9]. 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 [10, p 22]. There are several ways to apply internal controls within IS/IT security implementation such as Model of Corporate Governance Direct Control Cycle [11] and the use of General Deterrence Theory [12] and culture factor [13]. 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 [14], [15]. COSO is an example of an internal controls framework but is not exclusively used for guidance in IS/IT security practices and implementation [16]. COSO underlines the role of the board and senior management as the most needed component of a control structure [17], [18], [19]. The Sarbanes-Oxley Act was enacted covering internal controls, external financial disclosure, corporate governance and auditor behaviour[20]. 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 [21]. However, even though the Sarbanes-Oxley Act offers many benefits in US corporations today, there are some drawbacks.

III. 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 [22]. In other words, IS/IT security is the responsibility of corporate governance and the Board and senior management have oversight of those responsibilities.

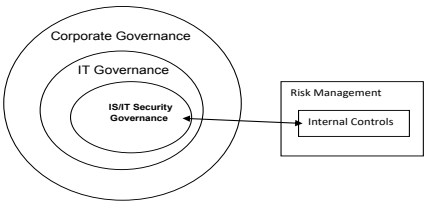

Fig. 1. Relationship between internal controls, risk management and IS/IT security governance

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 [23]. Recently, [24] 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 [25].

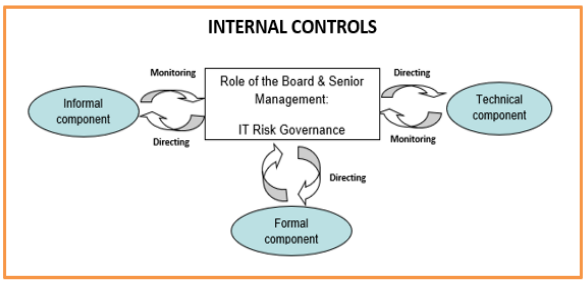

Fig.2. A conceptual framework of IT Security Governance and Internal Controls

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. 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 and 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 [11]. 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.

IV. Research Methodology

In this study, qualitative data were collected to answer both research questions. 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.

V. 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. During data analysis stage, fourteen themes have been identified from the Formal (n=8), Technical (n=3) and Informal (n=3) components respectively.

a) 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. 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. The following shows the evidence from business need category.

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 identified in the 2nd formal theme and 7th formal theme: *"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."*

b) 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 themes were identified, "techniques and controls", "system development" and "internet or network security". The following presents the interview data from technique and controls category:

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."*

c) 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. Three themes were identified: "staff integrity/ethicality/accountability", "culture/commitment" and "human issues-lack of awareness/stupidity". The following addresses the interview data from culture and commitment category, "*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".*

VI. Conclusion

Overall, 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. Interview data was used in the analysis. 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

REFERENCES

[1] Institute, I. G. (2006). "Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition."

[2] Baker, W. H. and L. Wallace (2007). "Is Information Security Under Control?" IEEE Security & Privacy: 36-44.

[3] Dhillon, G. and J. Backhouse (2000). "Information System Security Management in the New Millennium." Communications of the ACM 43(7): 125-128.

[4] OECD (1999). "Principles of Corporate Governance."

[5] Force, N. C. S. S. T. (2004). "Information Security Governance: A Call To Action."

[6] ITGI, I. G. I. (2003). "Board Briefing on IT Governance."

[7] Lin, P. P. (2006). "Systems security threats and controls." The CPA Journal, ABI/INFORM Global 76(7): 58.

[8] Dhillon, G., G. Tejay, et al. (2007). "Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations." Proceedings of the 40th Hawaii International Conference on System Sciences, IEEE.

[9] Solms, B. v. (2001). "Corporate Governance and Information Security." Computers & Security 20(3).

[10] Sinclitico, G. (2007). "Management Controls Have Finally Gone Away!" The Armed Frces Comptroller, Accounting & Tax Periodicals 52(2): 21.

[11] Solms, B. v. (2006). "Information Security- The Fourth Wave." Computers & Security 165-168.

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

[13] Labovitz, G. and V. Rosansky (1997). The Power of Alignment. New York, NY, USA, John Wiley & Sons, Inc.

[14] Varadharajan, V. (2007). "Researching Security in Organisations." EII Winter School, ARC Research Networks.

[15] Musa, N. & B Clift (2017). “Internal Control and Standard Operating Procedures in Malaysian Corporations”, Journal of Telecommunication, Electronic and Computer Engineering (JTEC) 9(2-10). ISSN: 2289-8131.

[16] Swanson, R. M. (1999). "Internal Controls: Tools, not hoops." Strategic Finance, ABI/INFORM Global 81(3).

[17] Bedell, D. (2006). "Security Complex." Global Finance 20(6): 25.

[18] Rogers, V. C., T. A. Marsh, et al. (2004). "Internal Controls: Winning the battle against risks." Internal Auditing, ABI/INFORM Global 19(4): 28.

[19] O'Leary, C., E. Iselin, et al. (2006). "The Relative Effects of Elements of Internal Control on Auditors' Evaluations of Internal Control." Pacific Accounting Review: Accounting & Tax Periodicals 18(2): 69.

[20] Boyle, G. and E. G.-. Webb (2007). "Sarbanes-Oxley and its Aftermath: A Review of the Evidence."

[21] Gordon, L. A., M. P. Loeb, et al. (2006). "The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities."

[22] OECD (2002) OECD Guidelines for the Security of Information Systems and Networks: Towards a culture of security.

[23] Baskerville, R. (1988). "Designing Information Systems Security." Information Systems Series, John Wiley.

[24] Yassine, Maleh & Zaydi, Mounia & Abdelkebir, Sahid & Ezzati, Abdellah. (2018). Building a Maturity Framework for Information Security Governance through An empirical study in Organizations. 10.4018/978-1-5225-5583-41.

[25] Mishra, S. and G. Dhillon (2007). "Information Systems Security Governance Research: A Behavioral Perspective." Annual NYS Cyber Security Conference.

[26] Veal, J. (2005). Business Research Methods: A Managerial Approach, Pearson Addison Wesley.