A Conceptual Framework of IT Security Governance and Internal Controls

Nadiatra 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 ethics.

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.