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