Internal Control and Standard Operating Procedures in Malaysian Corporations

Nadianatra Musa[1], Bob Clift[2]
[1]*Faculty of Computer Science and IT, Universiti Malaysia Sarawak, Kota Samarahan, Malaysia.*
[2]*School of Accounting and Corporate Governance, University of Tasmania, Hobart, Australia.*
nadia@unimas.my

***Abstract*—The security, standards, and related controls of IT/IS infrastructure along with its implementation in Malaysian Corporation has been the main focus of the study. A cross sectional analysis has been implemented, using the qualitative research design, to evaluate the importance of internal control and standard operating procedures. The interview data, website analysis, and mail surveys have been collected concerning the perfection of boards and senior management about the IS/IT security processes. Both the senior and board management are ought to be responsible and accountable to ensure that IS/IT risks are addressed in the standards and policies of IS/IT security. Success and failure of development are also the responsibility of boards and senior management. IT/IS procedures must be implemented by corporation to control the risk related with the use of operation and information systems that supports the mission of business.**

***Index Terms*—Board Management; IS/IT;Security; Senior Management.**

I. INTRODUCTION

In most of the countries, the corporate rules and principles about the responsibilities and power of the corporations are mainly related to theboard of directors [1]. It is apparently known that incompetence within the association and tolerance for dishonesty is observed as negligence [2]. There is a series of management models, standards, and case laws, suggesting the procedures and ways to the board of directors for operating the system. The interest of the study lies in the role of IT/IS that fits into the model of governance. The study has been designed in a manner that emphasizes the responsibilities,potential and role of IT/IS, which can contribute in developing the best outcomes for the interest of corporation [3]. The development of IT/IS model for the security governance might contribute to the decision of turf war that may enhance the practice of governance. The model is expected to provide with a structure for the advances of more general corporate governance framework that is presumed to be helpful for the organizations, using computers [4].

The literature has not presented any study that may have discussed the involvement of senior managements and the board of directors in IT/IS security governance among public listed companies in Malaysia. Eventually, no understanding has been found in the interaction of IT/IS security issues among the senior managers and other line managers. There are evidences that the major incidents and the failures of security in IS/IT were triggered by the staff members. For instance, it has been observed that many employees do not bring their problems,concerning the security of IS/ITto the observance of HODs or departments for many possible strategic policies [5]. The literature has suggested that incompetency of the senior managers and the boards with regard to the security problems related to the IS/IT may lead to ineffective security controls.

Threats and susceptibility have been identified as the major causes of the security issues. Yet, the Malaysian corporation has still not recognized the ways by which these susceptibilities and threats can be controlled [6]. The understanding to control these incidents is strongly encouraged as it can mark positive impact on supporting and protecting the IS/IT business information and assets. It is well known that if the business assets and information about IS/IT of the organization are exploited and remain in a susceptible state, they can lead to the failure of availability and integrity in the system [7]. If the integrity, availability, and confidentiality of business information are negotiated, corporations might incur indirect and direct losses to the business. For instance, in the case of Arthur Anderson, the commodity and service company, Enron and its auditor, the senior management was represented to be involved in the establishment of 'off-balance sheet' activities that helped to enhance the performance financially and increased the stock prices [8]. These evidences have represented that fraudulent behavior has been the key factor that lead to the fall of Enron (Services Company).Human error was also one of the main issues of Enron fall as it was presumed that the senior managers and board were incapable to recognize and defend the security threats and vulnerabilities, which lead to various security attacks [9].

A company, having IT/IS security control and standards, does not mean that IT/IS will be well mannered and managed as previously suggested by Baker, et al. [10]. Many past studies haveconcentrated on the absence and presence of security procedures and controls; however, limited focus has been directed to the quality of implementation. Baker et al. developed a web survey to generate a better understanding of the ways IS/IT procedures have been implemented to manage the security risks of assets and business.The web survey addressed 16 categories of general security domains. These security domains were intended to cover three components of formal, informal and technical elements. For example, the controls of antivirus software, like back-up and recovery, has been identified as a technical component. Business continuity and incident response were the examples of general security control domains for the formal component. Among all the 16 categories, none of them presented any informal component exclusively. It has been presumed that the informal component has been opted within the execution of both technical and formal components.

The study also aimed to explore the likelihood of a more