An Evaluation of Security Governance Model in Organizational Information Technology or Information Systems Security Implementation

Dayang Hanani Abang Ibrahim, Nadianatra Musa, Chiew Kang Leng
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak
hananii@unimas.my

***Abstract*—The study was aimed to investigate the security governance model in organizational IT security implementation. A triangulate design has been applied to data collection from three sources websites, interviews, and survey. Automatic security measures controls have been adopted to minimize and control the human actions and the correspondence with the system. Important elements depicted from the findings include directing and monitoring actions within the IS/IT security. The IS/IT security governance model of the inter relationship among the three components of the Formal, Technical and the Informal are important to achieve the good practices of IS/IT security. The educational concept may also increase the organisational and the employee values. The study has affirmed positive prevalence of the trend that most of the companies are now considering to implement IT/IS security models for protected data.**

***Index Terms*—Data; Information; IS/IT; Model; Security; Threat;**

I. INTRODUCTION

Security governance as a system refers to a rule conceived by corporate performers and individuals targeting at managing, coordinating and regulating the overall existence in regards to threats to their ontological and physical security. The ruling systems chiefly depend on the political authorities of agreed-upon institutions, practices, and norms as well as on the technologies, spatial forms, rationalities and identities across which transnational and international security activity takes place. In the present study, the security practices have been discussed along with their mechanisms from which they are derived.

The self-interest of organization can be enlightened by implementing the effective IT security program. Companies are taking serious actions to preserve their information commended to them by suppliers, customers, and their partners. They are maintaining the responsibility for the companies' security plans and adopting the programs to address and evaluate the internal and external threats and vulnerabilities of the economic information.

Mechanisms of the security governance are apparently delineated set of norms, rules, and practices that coordinate the security associations in the International system between performers. The association between the norms and individuals that motivate specific mechanisms of security governance is constantly and mutually re-enacted. The State or city-states (units) may constitute the mechanism of the power of balance through the practices. This mechanism constitutes this unit in a specific relationship based on sovereign *deterrence* and independence. Concerning the rising abundance of regulations, rules, and guidelines, it becomes apparent that information security is not just a technical issue, but it is an organizational governance challenge. Increased scrutiny is being faced by the businesses today when it comes to accountability, ethics, and governance.

Lack of involvement by the board and senior management in understanding the IS/IT security issues and improper implementation plan of IS/IT security within the formal, informal and technical components has led the study to focus on the evaluation of security governance model. It might be important to focus on the limited internal control applications over IS/IT security. The gaps in the literature have led to the development of two important research questions, which have driven the development of the conceptual framework and the model of IT/IS security governance:

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

Question 2: How can directing and monitoring actions in the technical, formal and informal components of IS/IT security governance in corporations be implemented effectively and efficiently?

The conceptual framework has been extended by incorporating the security governance model, which suggests various areas regarding the elements of the three components formal, technical and informal and component interactions (Relationship Type 1-Formal/Informal, Relationship Type 2-Formal/Technical and Relationship Type 3-Technical/Informal) within Malaysian Publicly Listed Corporations. The risk management and internal control practices are ought to be included in the IS/IT security according to the suggested model, through monitoring and directing actions. It also emphasizes the relationship between the holder and supervisor of the responsibility. Because the nature of the study is confidential and sensitive so, the study has opted a triangulation method to eliminate the research gap.

The study has contributed to enhance the IS/IT security governance process, which is a complicated task and requires the giver/supervisor and the holder of the responsibility to resolve the issues in an effective and efficient way at minimum risk. Failure to understand the responsibilities in discharging IS/IT security may bring the