A model of component interaction between Formal, Technical and Informal components within IS/IT security governance

Nadianatra Musa
Department of Information Systems
Faculty of Computer Science and IT,
Universiti Malaysia Sarawak
Kota Samarahan, Malaysia
nadia@fit.unimas.my

Bob Clift
School of Accounting and Corporate Governance
University of Tasmania
Hobart, Australia
bob.clift@optusnet.com.au

***Abstract*—In most countries, corporate statutes and rules (mandatory or voluntary) about powers and responsibilities in corporations (corporate governance) place responsibility on the Board of Directors acting as a Board. However, these documents do not provide much guidance about recognizing potential problems or about preventative measures. Even so, it is apparent that knowingly tolerating dishonesty or incompetence within the corporation is likely to be regarded as negligence. Most organizations today pay little attention to the inter-relationship between the Formal component, Technical component and Informal component. The Board and senior management of organizations tend to focus more on narrow aspects such as IS/IT management rather than on a comprehensive view. Deficiencies in any of these three components may result in unbalanced IS/IT security implementation. The objective of this study is to integrate the three components simultaneously throughout the IS/IT security implementation. The model of IS/IT security governance is a comprehensive conceptual framework because it emphasizes the two-way relationship between each of the components. In this study, a triangulated approach is adopted, data were collected in three phases, phase 1 is a website analysis, phase 2 is an interview and phase 3 is a mail survey. The interactions of three components, formal, technical and informal are significant in the IS/IT security governance model.**

Keywords- IT security governance; Formal component; Technical component and Informal component component;

I. INTRODUCTION

Over the past forty years or so, computers have replaced many of the manual systems of recording the activities of business and governmental organisations all over the world. More recently, the advances in technology have admitted millions of users to the Internet which has changed the environment in which our economic, social and political activities are conducted. One outcome of these changes is the massive publicity that follows the discovery of any fraud in either the public or private sector and the occurrence of any technical break-down in computer systems, for example, in the reports and post-event analyses of such frauds as Enron and etc [1] it was never made absolutely clear whether these events were triumphs of outright dishonesty or whether the existing regulatory and recording systems were flawed which made it easier for the perpetrators to operate their schemes. Several corporate disasters received world-wide publicity and have stimulated research in many disciplines ranging from philosophy to labour relations but this investigation has been prompted by the confusion in the literatures relating to the business disciplines and Information Technology/Information Systems (IT/IS).

Some protagonists claim that the Board of Directors is responsible for the detailed operation of the computer systems and, therefore, must ensure that Board members are aware of what is going on and establish policies and procedures to ensure that the systems operate as planned. Other protagonists take the view that system designers, programmers and IT staff ought to be sufficiently well informed about the specific business environment to be able to advise the Board about potential problems and currently available solutions.

Overall, the literature reflects a mixture of blame-shifting and lack of knowledge about what and why others in the organisation are required to do and how performance is monitored. At one level, this could be described as competition for status among different groups of employees. At another level, it could be seen as the lack of a theory which identifies problems, responsibilities and relationships among the various groups.

In most countries, corporate statutes and rules (mandatory or voluntary) about powers and responsibilities in corporations (corporate governance) place responsibility on the Board of [Directors acting as a Board [2][3] However, these documents do not provide much guidance about recognising potential problems or about preventative measures. Even so, it is apparent that knowingly tolerating dishonesty or incompetence within the corporation is likely to be regarded as negligence.

Most organisations today pay little attention to the inter-relationship between the Formal component, Technical component and Informal component [4][5][6][7]. The Board and senior management of organisations tend to focus more on narrow aspects such as IS/IT management rather than on a