Chapter XXI
A Model of Information Security Governance for E-Business

Dieter Fink
Edith Cowan University, Australia

Tobias Huegle
Edith Cowan University, Australia

Martin Dortschy
Institute of Electronic Business–University of Arts, Germany

ABSTRACT

This chapter identifies various levels of governance followed by a focus on the role of information technology (IT) governance with reference to information security for today's electronic business (e-business) environment. It outlines levels of enterprise, corporate, and business governance in relation to IT governance before integrating the latter with e-business security management. E-business has made organisations even more reliant on the application of IT while exploiting its capabilities for generating business advantages. The emergence of and dependence on new technologies, like the Internet, have increased exposure of businesses to technology-originated threats and have created new requirements for security management and governance. Previous IT governance frameworks, such as those provided by the IT Governance Institute, Standards Australia, and The National Cyber Security Partnership, have not given the connection between IT governance and e-business security sufficient attention. The proposed model achieves the necessary integration through risk management in which the tensions between threat reduction and value generation activities have to be balanced.

INTRODUCTION

Governance has gained increasing attention in recent years, primarily due to the failures of well-known corporations such as Enron®. The expectations for improved corporate governance have become very noticeable, especially in the

United States, where the Sarbanes-Oxley (SOX) Act of 2002 aims to restore investor confidence in U.S. markets by imposing codes of conduct on corporations. The concept of corporate governance is much quoted as "the system by which companies are directed and controlled" (Cadbury, 1992, p.15). The corporate governance structure, therefore, specifies the distribution of rights and responsibilities among different participants in the corporation, such as the board of directors and management. By doing this, it provides the structure by which the company objectives are set and the means of attaining those objectives and monitoring performance.

Corporate governance includes concerns for information technology governance because without effective information management, those charged with corporate responsibilities would not be able to perform effectively. *eWeek* (2004) make the case for IT professionals to take a leading role in corporate governance since they have control over the processes underpinning governance activities. They mention the example of the human resource database providing information about employees' compensation which, if the information is properly monitored, could provide an early indication of malpractice. This means that IT functions need to be secure so that "business data is not altered by unscrupulous hands" (*eWeek,* 2004, p. 40). With business increasingly utilising modern digital technology in a variety of ways, effective information security governance has, therefore, become a key part of corporate governance.

In this chapter, the role of corporate governance in relation to the security of information technology and *information and communications technology* (ICT) will be examined. Current developments and models such as those offered by the IT Governance Institute and Standards Australia will be outlined and the current lack of model development in extending the governance concept to information security in today's world of e-business will be identified and discussed. The purpose of the chapter is thus to develop a model that aligns IT governance with security management in an e-business environment through a review of existing approaches and synthesis of concepts and principles.

NEED FOR GOVERNANCE

The case of Enron® exemplifies the need for effective corporate governance. Enron®'s downfall was brought about, as described in broad terms by Zimmerman (2002) in USA TODAY®, by "over-aggressive strategies, combined with personal greed." He believes that there were two main causes for this failure: first, breakdowns caused by ignored or flawed ethics, and second, "Board of directors failed their governance." He recommends that in order to keep this from happening again, corporate governance should no longer be treated as "soft stuff," but rather as the "hard stuff" like product quality and customer service. He quotes *Business Week*® of August 19-26, 2002 when he concludes that "a company's viability now depends less on making the numbers at any cost and more on the integrity and trustworthiness of its practices." In other words, good corporate governance.

The term corporate governance is often used synonymously with the term enterprise governance since they are similar in scope as can be seen from the following definitions. They both apply to the role and responsibilities of management at the highest level in the organisation. An example of a framework for enterprise governance is one that is provided by the *Chartered Institute of Management Accountants* (CIMA) and the *International Federation of Accountants* (IFAC) (2004):

[Enterprise governance is] the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly.