IDEA GROUP PUBLISHING **ITB12224**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, Enterprise Information Systems Assurance and Systems Security
edited by Merril Warkentin © 2006, Idea Group Inc.

Chapter II

IT Security Governance and Centralized Security Controls

Merrill Warkentin, Mississippi State University, USA

Allen C. Johnston, University of Louisiana-Monroe, USA

Abstract

Every enterprise must establish and maintain information technology *(IT) governance procedures that will ensure the execution of the firm's security policies and procedures. This chapter presents the problem and the framework for ensuring that the organization's policies are implemented over time. Since many of these policies require human involvement (employee and customer actions, for example), the goals are met only if such human activities can be influenced and monitored and if positive outcomes are rewarded while negative actions are sanctioned. This is the challenge to IT governance. One central issue in the context of IT security governance is the degree to which IT security controls should be centralized or decentralized. This issue is discussed in the context of enterprise security management.*

Introduction

Information system security management goals can only be achieved if the policies and procedures are complete, accurate, available, and ultimately executed or put into action. Organizations must be conscious of the hazards associated with the diffusion of

technology throughout the firm and must reflect this awareness through the purposeful creation of policy. Furthermore, it is prudent that organizations take the appropriate measures to maximize the transfer of policy into effective security management practices. This can only happen with an effective organizational design or structure and with adherence to proper information assurance procedures. Stakeholder compliance is only possible with the enforcement of internal controls to ensure that the organization's policies and procedures are executed.

The goals of IT security are to ensure the confidentiality, integrity and the availability of data within a system. The data should be accurate and available to the appropriate people, when they need it, and in the appropriate condition. Perfect security is not feasible — instead IT security managers strive to provide a level of assurance consistent with the value of the data they are asked to protect.

It is within their structures and governance procedures that organizations are able to address the issues of responsibility, accountability, and coordination toward the achievement of their purpose and goals. As organizations evolve to position themselves appropriately within their domains of interest, their governance posture evolves. These changes are reflected in the IT component of the organization as well. Within this mode of flux, however, one thing remains constant — a desire to obtain and maintain a high level of information assurance. In this context, the roles of IT governance and organizational design in fulfilling the security management commitment are presented and presented.

Policies-procedures-practice. An organization's information security is only as good as the policies and procedures designed to maintain it, and such policies and procedures must also be put into practice (or executed). If managers, developers, and users are not aware of such policies and procedures, they will not be effectively executed. Of critical importance to the assurance of information security is the establishment of an enterprise training program with verifiable training protocols to ensure that all personnel (new and existing) are fully aware of such polices and procedures so that they can be put into practice on a daily basis.

Figure 1. Security policy — procedure — practice