Chapter II

Information Systems Security and the Need for Policy

Michael E. Whitman
Kennesaw State University

Anthony M. Townsend
University of Delaware

Robert J. Aalberts
University of Nevada, Las Vegas

As the pervasiveness of networks create a more open set of information systems for the mobile and diverse needs of the organization, increased attention must be paid to the corresponding increase in exposure of those systems to attacks from internal and external sources. The first step to preparing the organization against these threats is the development of a systems security policy which provides instruction for the development and implementation of a security posture, as well as provides guidelines for the acceptable and expected uses of the systems. This chapter provides background support for the need for information security policy, and outlines a sample structure that may be used to develop such a policy.

INTRODUCTION

In 1999 financial losses due to breaches in computer security amounted to over $100,000,000 for the third straight year. Respondents in the 1999 CSI/FBI survey reported a total of $123,779,000 in losses (CSI, 1999). The most serious financial

This chapter appears in the book, *Inforamtion Security management: Global Challenges in the New Millennium* edited by Gurpreet Dhillon. Copyright 2001, Idea Group Inc.

losses occurred through theft of proprietary information, which poses perhaps the greatest threat to U.S. economic competitiveness in the global marketplace. In an effort to help combat information theft, firms indicated that encryption was the primary type of security technology planned for purchase in 1998 (CSI, 1997). Computer crime consisting of Hardware/Software theft was fifth on Pinkerton's list of top 10 threats, while computer crime through Internet/Intranet security lapses was rated seventh (Pinkerton's, 2000).

The three basic elements of security are access control, authentication and accounting (Cantin, 1999). Although encryption systems, access protections and the like are the most visible components of effective system security, protecting the firm against theft of proprietary information and from other forms of computer-based financial crimes and vandalism really begins with comprehensive information system security policy. Even the best security systems can be compromised if they are not used properly; well-written and rigorously enforced system use policy focusing on the three basic goals of security: confidentiality, integrity and availability will ensure maximum protection in return for the firm's security investment (Clyde, 1999). The first priority in systems security is the establishment of security policy (SANS, 2000; Sword & Shield, 1999).

Threats to information systems security are as varied as the systems themselves (Fitzgerald and Dennis, 1999; Loch et al. 1992). While some security issues are common to most organizations, others are idiosyncratic to individual organizations or industry groups. As such, there is no "out of the box" security response (nor attendant policy) that truly fits all organizations.

A security policy has been defined as "the set of laws, rules, and practices regulating how an organization manages, protects, and distributes sensitive information" (Walker, 1985). It is "a wide ranging document which is about managing the business as a whole, managing it securely and protecting a company's key asset - its information" (Woodward, 2000). Policies differ greatly between organizations depending on the value and sensitivity of information to be protected, as well as the potential effects of damage, modification or disclosure of the information to the organizational well-being (Steinke, 1997). Generally speaking, the eventual system security policy will address a number of distinctly different issues; first, good security policy will address the security of the physical plant itself; policy must help secure the functional aspect of the system (i.e., data integrity, access, etc.); finally, policy must address procedures to protect the system from external threats and piracy. All of these areas of concern, if ignored can lead to significant financial loss to the organization. Thus, formalizing systems security through an effective policy is a critical step an organization must take to ensure system integrity. Beyond codifying system security procedures, policy must be designed to support organizational goals, without creating undue restrictions on operational functionality. There is a fine balance between security and access. Perfect security inevitably results in virtually no access. Complete access similarly results in a total lack of security. Security becomes more of a balancing process in which the security managers attempt to determine what level of IN-security the organization is willing to live with in order to provide sufficient access to organization information as needed by its employees.