Chapter I

Security Risk Assessment and Electronic Commerce: A Cross-Industry Analysis

Jonathan W. Palmer
University of Maryland, USA

Jamie Kliewer and Mark Sweat
University of Oklahoma, USA

The security issue has been a compelling one for many organizations. In two separate studies completed in April 1998, Fortune 100 companies reported more financial losses due to computer vandalism and espionage in 1997 than they ever experienced before. Several corporations said they lost $10 million or more in a single break-in. And reports of system break-ins at the Computer Emergency Response Team site are the highest they’ve ever been.

Management objectives for security reflect the individual organization’s situation. However, there are several common themes in the objectives for security:

• Safeguarding the organization’s assets and resources.
• Complying with policies, procedures, laws, and regulations.
• Utilizing resources economically and efficiently.
• Ensuring the reliability and integrity of information.

Billions of bits of information are being transferred and maintained daily throughout the world. These facts combined with trends toward a greater use of virtual organizations, electronic data interchange with trading partners, and the outsourcing of information...
handling have proven the effectiveness and profitability of electronic commerce. Consequently, the shift to a computer mediated business environment has opened up several new security gaps in important industrial information. Vast amounts of information can be stolen or tampered with in just a matter of seconds. In addition, companies are facing new security issues regarding sharing of information; preventing unwanted intrusions; and avoiding unintentional mistakes.

More than a million systems are now connected to the Internet, and approximately 50 million people in 100 countries from all seven continents use Internet services (U.S. Department of Commerce, 1997). Currently, the most common use of the Web is for e-mail and advertisement; however, the Internet is quickly becoming a common communication tool in business, the average businessperson is quite familiar with many of the other benefits the Internet offers. As an extension of their Internet use, many companies have implemented their own intranets and have often experienced substantial improvements in information flow, performance, collaboration, teamwork, and customer-responsiveness.

The Internet offers many potential advantages, increases the level of business with current customers, helps to find new customers, and helps to conduct business at a lower cost. However, without adequate security, the Internet involves many risks. Using the Internet for communication and advertising still necessitates isolating the corporate network to protect internal information. More firms are extending their network to include various forms of electronic commerce. Most often, electronic commerce transactions entail computer connections between known parties—various vendors, customers, and trading partners—however, without proper security in place, neither party can be certain of the transmission’s authentication or content.

This chapter examines security issues across multiple organizations, focusing on the security concerns in an internetworked environment. The chapter examines current threats facing organizations including alteration, denial of service, errors and omissions, system malfunctions, fraud or theft, unauthorized disclosure, and regulatory and contractual exposure. Basic solutions necessary to minimize or control the damage are also identified. This topic is approached through three levels: Internal, Business to Consumer, and Business to Business. A survey of 35 individuals across four industries (telecommunications, energy, retail, and the public sector) provides the basis
Firewall Rulebase Management: Tools and Techniques
www.igi-global.com/chapter/firewall-rulebase-management/52947?camid=4v1a