IDEA GROUP PUBLISHING **ITB13043**

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, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos

Chapter X

Incident Preparedness and Response: Developing a Security Policy

Warren Wylupski, University of New Mexico, USA

David R. Champion, Slippery Rock University, USA

Zachary Grant, New Mexico Mounted Patrol, USA

Abstract

One of the emerging issues in the field of digital crime and digital forensics is corporate preparedness in dealing with attacks on computer network security. Security attacks and breaches of an organization's computer network can result in the compromise of confidential data, loss of customer confidence, poor public relations, disruption of business, and severe financial loss. Furthermore, loss of organizational data can present a number of criminal threats, including extortion, blackmail, identity theft, technology theft, and even hazards to national security. This chapter first examines the preparedness and response of three southwestern companies to their own specific threats to corporate cyber-security. Secondly, this chapter suggests that by developing an effective security policy focusing on incident detection and response, a company can minimize the damage caused by these attacks, while simultaneously strengthening the existing system and forensic processes against future attacks. Advances in digital forensics and its supporting technology, including intrusion detection, intrusion prevention, and application control, will be imperative to maintain network security in the future.

Introduction

On 12 April 2005, LexisNexis acknowledged that personal information on as many as 310,000 U.S. residents may have been stolen from its databases. The company had announced in March that information on approximately 30,000 persons had been stolen, but an internal investigation increased the estimate. LexisNexis is informing affected individuals by mail that they may be at risk of identity theft from unknown persons who illegally accessed the passwords and identity information of legitimate customers of Seisint, which LexisNexis bought in September 2004. (Litan, 2005)

Information is crucial. Those armed with information have the ability to do great good or cause great harm. Corporations and organizations that harbor personal, sensitive, or proprietary information can no longer take a passive approach to computer network and data security. Even while companies strive to apply the evolving field of digital forensics to their overall network security, external and internal threats to corporate cyber-security have grown tremendously. External threats consist of *malware* such as *viruses* and *Trojan horses*, *spyware*, and *adware*. Malware is malicious software that designed to disrupt or damage systems. Other external threats include, *script kiddies*, *social engineering*, *spam*, and *hacking*. (See Table 1 for definitions of these terms.) Internal threats stem from disgruntled employees and non-compliant (non-malicious) employees. These activities can lead to a loss of network integrity and loss of data. Worse, criminals can use proprietary organizational data for a number of dangerous or illegal activities, including extortion, fraud, theft or national security threats.

Attempted computer intrusion has become a common occurrence for businesses, regardless of their size or nature of their industry. Even the familiar and ubiquitous e-mail venue has become a thoroughfare for malicious entry into organizations. One southwestern healthcare company receives over 70,000 e-mail messages a month, of which 17,000 are legitimate messages, while the others are spam. Another southwest organization estimated that 70% to 75% of the incoming e-mail was unwanted. While most of these e-mail messages cause no harm, the cost to prevent a breach in computer security from this and other methods increases every year, according to Ware (2004).

Additional security challenges can come from the installation of wireless routers, unauthorized downloads and installation of software, and the loss and theft of computer desktops, laptops, and portable storage media. Loss of hardware or storage media can cause considerable damage to an organization's reputation. In 2005, Bank of America disclosed that in late December 2004 it lost unencrypted computer backup tapes containing Social Security numbers and other personal data belonging to government employees based on 1.2 million federally issued credit cards. At the time of the announcement, there was no evidence that any fraudulent activity had occurred due to information that existed on those tapes. In 2001, the Federal Bureau of Investigation announced that it was missing 184 laptop computers; three computers held information considered sensitive, and one computer held confidential information (Weyden, 2001).

Given the increase in intensity and severity of system intrusion attempts, most organizations today are without sophisticated protection systems or an effective security