Carnegie Mellon
Software Engineering Institute

Insider Threat Study:
Computer System Sabotage in Critical Infrastructure Sectors
Executive Summary

Michelle Keeney, J.D., Ph.D.
Eileen Kowalski
National Threat Assessment Center
United States Secret Service
Washington, DC

Dawn Cappelli
Andrew Moore
Timothy Shimeall
Stephanie Rogers
CERT® Program
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA

May 2005

Background

Securing American cyberspace has become a national priority. In *The National Strategy to Secure Cyberspace*[1], the President's Critical Infrastructure Protection Board emphasizes the importance of public-private partnerships in securing the Nation's critical infrastructures and improving national cyber security. Similarly, one focus of the Department of Homeland Security is enhancing protection for critical infrastructure and networks by promoting working relationships between the government and private industry. The federal government has acknowledged that these relations are vital because most of America's critical infrastructure is privately held.

The nation's dependence on interconnected networks and communications systems significantly increases the risk of harm that could result from the activities of insiders. In addition, the actions of a single insider can cause extensive financial damage or irreparable damage to an organization's data, systems, business operations, or reputation. Examination of the prevalence of insider activity across critical infrastructure sectors, the motives of insiders, their methodologies, and identification of the behaviors and activities of insiders may help to prevent future insider incidents and improve cyber security. In particular, research on this issue may arm private industry, government, and law enforcement with strategies to assess potential threats to, and vulnerabilities in, data and critical systems.

The Secret Service has a duel mission of protection and investigations. They are mandated to investigate financial criminal activity in the prevention of electronic crimes. In support of their protection mission, the Secret Service has a vested interest in identifying and mitigating vulnerabilities to information systems that could impact physical security.

---

[1] The National Strategy to Secure Cyberspace. (February 2003). http://www.whitehouse.gov/pcipb/.

Carnegie Mellon
Software Engineering Institute

The CERT Coordination Center, located at Carnegie Mellon University's Software Engineering Institute, coordinates responses to security compromises, identifies trends in intruder activity, identifies solutions to security problems, and disseminates information to the broader community. CERT conducts research and development to create solutions to security problems and provides training to help individuals build skills in dealing with cyber-security issues.

Since 2002, the Secret Service and CERT have collaborated on an effort to examine the issue of insider cyber activity, the Insider Threat Study. This effort was spearheaded by concern over the ability of insiders to exploit known system vulnerabilities and the effect of this activity on organizations, particularly those within critical infrastructures.

The Insider Threat Study

The insider Threat Study (ITS) was designed to analyze these incidents from both a behavioral and a technical perspective. The cases examined in the Insider Threat Study are incidents perpetrated by insiders (current or former employees or contractors) who intentionally exceeded or misused an authorized level of network, system, or data access in a manner that affected the security of the organizations' data, systems, or daily business operations. Cases involved incidents that have occurred in critical infrastructure sectors between 1996 and 2002.

The ITS consists of several components:

- an aggregated case-study analysis that provides an in-depth look at insider incidents that have occurred in critical infrastructure sectors between 1996 and 2002.
- a review of the prevalence of insider activity across critical infrastructure sectors over a 10-year time frame
- a survey of recent insider activity experienced by a sample of public- and private-sector organizations[2]

The first report from the aggregated case study analysis, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,* focused on cases within the Banking and Finance Sector and was published in August 2004.[3] This report, *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors,* is the second of the series. It reports on the examination of forty-nine insider incidents across critical infrastructure sectors in which the insider's primary goal was to sabotage some aspect of the organization (for example, business operations, information/data files, system/network, and/or reputation) or direct specific harm towards an individual.

Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors

Research for this report found that the majority of the insiders who committed acts of sabotage were former employees who had held technical positions with the targeted organizations. As a result of their involvement in the incidents reviewed for this study, almost all of the insiders were charged with criminal offenses. The majority of these charges were based on violations of

[2] 2004 E-Crime Watch Survey.
[3] Available on-line at http://www.cert.org/archive/pdf/bankfin040820.pdf and http://www.secretservice.gov/ntac_its.shtml

Carnegie Mellon
Software Engineering Institute

federal law. The key findings from this study of insider sabotage across critical infrastructure sectors are the following:

- A negative work-related event triggered most insiders' actions.
- Most of the insiders had acted out in a concerning manner in the workplace.
- The majority of insiders planned their activities in advance.
- When hired, the majority of insiders were granted system administrator or privileged access, but less than half of all of the insiders had authorized access at the time of the incident.
- Insiders used unsophisticated methods for exploiting systemic vulnerabilities in applications, processes, and/or procedures, but relatively sophisticated attack tools were also employed.
- The majority of insiders compromised computer accounts, created unauthorized backdoor accounts, or used shared accounts in their attacks.
- Remote access was used to carry out the majority of the attacks.
- The majority of the insider attacks were only detected once there was a noticeable irregularity in the information system or a system became unavailable.
- Insider activities caused organizations financial losses, negative impacts to their business operations and damage to their reputations.