Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector

Executive Summary

January 2008

Introduction

Securing American critical infrastructures is a national priority. In *The National Strategy to Secure Cyberspace,* the President's Critical Infrastructure Protection Board emphasizes the importance of securing the nation's critical infrastructures and improving national cyber security. As most of America's critical infrastructure is privately held, a key component of the strategy is strengthening public-private partnerships. Similarly, the U. S. Department of Homeland Security is engaged in initiatives to enhance protection for critical infrastructure and networks by promoting working relationships between the government and private industry. One of these initiatives specifically promotes awareness of the insider threat issue to organizations.

The insider threat is a problem faced by all industries and sectors today. The consequences of insider incidents can include lost staff hours, negative publicity, and financial damage so extensive that a business may be forced to lay off employees or close its doors. Furthermore, insider incidents can have repercussions extending beyond the affected organizations to include disruption of operations or services within critical sectors, or the issuance of fraudulent identities that create potential risks to the public and homeland security.

This report presents the findings of a research effort to examine reported insider incidents within the Information Technology and Telecommunications (IT) sector. This effort is part of a larger research initiative, the Insider Threat Study (ITS), a collaborative endeavor of the United States Secret Service's National Threat Assessment Center (NTAC) and the CERT® Program (CERT) of Carnegie Mellon University's Software Engineering Institute. The study stems from concern about the ability of employees with intent to exploit known system vulnerabilities and the effect of their activities on organizations, particularly those within critical infrastructure sectors.

Overview of the Insider Threat Study

Initiated in 2002, the ITS is an exploration of employees who perpetrated acts of harm against organizations via computer, system, or network to include theft of intellectual property, fraud, and acts of sabotage within critical infrastructure sectors. The overall objective of the ITS is to

help private industry, government, and law enforcement better understand, detect, and possibly prevent harmful insider activity. A particular focus of the study is to identify information that may have been discernable prior to the incident from both a behavioral and technical perspective.

The ITS consists of the following components:

- An annual survey to estimate the prevalence of insider activity experienced by a sample of public and private sector organizations;
- Several in-depth case study analyses of insider incidents that occurred within the banking and finance, information technology and telecommunications (IT), and government critical infrastructure sectors; and,
- An aggregate analysis of insider incidents across the critical infrastructure sectors where sabotage was the goal or intent.

This report on illicit insider cyber activity in the IT sector is third in a series of findings from this multi-year research effort. Previous reports from the study include: *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,* an examination of incidents within the Banking and Finance Sector, published in August 2004; *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors,* an examination of sabotage incidents across critical infrastructure sectors, published in May 2005; and, *Insider Threat Study: Illicit Cyber Activity in the Government Sector,* an examination of incidents within federal, state, and local government agencies, published in January 2008.

The cases examined in the ITS involve incidents perpetrated by current, former, or contract employees who intentionally exceeded or misused authorized levels of computer, system/network, or data access in a manner that affected the organizations. Only those cases meeting these inclusion criteria that occurred within the United States between 1996 and 2002, in an organization that fell within a critical infrastructure sector, were included in the study.

Insider Threat Study: Illicit Cyber Activity in the IT Sector

This ITS report examines 52 incidents carried out by 57 insiders that occurred in the information technology and telecommunications sector (IT) between 1996 and 2002. Of the 52 incidents, 24 involved solely sabotage; 11 involved solely theft of intellectual property; 8 involved solely fraud; 6 involved both sabotage and theft of intellectual property; and 3 involved both fraud and theft of intellectual property.

Organizations affected by insider activity in this sector included

- internet service providers
- companies conducting e-business
- software, hardware, network, and telecommunication equipment manufacturers and suppliers
- newspapers
- companies that provide information technology and telecommunications-related technical consulting services

Key Findings

- Current and former employees carried out insider activities in nearly equal numbers.

- Sixty-three percent of the insiders held technical positions within the targeted organizations.
- Thirty-eight percent of insiders had prior arrests.
- A specific work-related event triggered most (73%) insiders' actions.
- The majority (76%) of insiders planned their activities in advance.
- Half (50%) of the insiders had authorized access to the system/network at the time of the incident.
- Over half (58%) of the insiders used relatively sophisticated tools or methods for their illicit activities, including scripts or programs, autonomous agents, toolkits, probing, scanning, flooding, spoofing, compromising computer accounts, or creating unauthorized backdoor accounts.
- Insiders committed their illicit activities both from the workplace (51%) and remotely (43%) in nearly equal numbers.
- The incidents took place during (51%) and outside (49%) normal working hours in nearly equal numbers.
- Most (80%) of the insider incidents were only discovered through manual (non-automated) detection of an irregularity or failure of an information system.
- The majority (74%) of the insiders took steps to conceal their identities and their activities.

Study Limitations

It is unknown whether the cases studied here are representative of all insider activity within organizations, including government agencies. Private organizations may be reluctant to report incidents of illicit cyber activity, even to law enforcement, suggesting that the actual number of insider cases may be significantly greater than those to which ITS researchers had access. Nevertheless, limitations associated with the number of cases examined by the ITS do not diminish the value of the knowledge that can be gained from analyzing these incidents. The study findings provide insights into actual illicit acts committed by insiders that may be useful to those individuals in the sectors charged with protecting critical assets as they begin to examine ways of improving their defense against insider attacks.

About the United States Secret Service

The Secret Service has a dual mission of investigation and protection. It is mandated to investigate financial criminal activity in the prevention of electronic crimes. In addition, the Secret Service has taken a lead role in the developing area of cyber crime, establishing working partnerships in both the law enforcement and business communities to address such issues as protection of critical infrastructure, internet intrusions, and associated fraud. In support of the protective mission, the Secret Service has a vested interest in identifying and mitigating vulnerabilities to information systems that could impact physical security.

The National Threat Assessment Center is a part of the Secret Service's Intelligence Division, and was created in 1998 to provide leadership and guidance to the emerging field of threat assessment. Two previous NTAC studies, the Exceptional Case Study Project and the Safe School Initiative, analyzed physical attacks on public officials and public figures and attacks on schools. Both studies focused on identifying information that was operationally relevant and that could help prevent future violent or disruptive incidents. Findings from the Insider Threat Study

may similarly enhance efforts within law enforcement, corporate security, information technology, and others in prevention, early detection, and investigation of cyber-related crimes.

About CERT

CERT is located at Carnegie Mellon University's Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania, USA. The SEI is a U.S. Department of Defense sponsored federally funded research and development center. The CERT Coordination Center, an initiative within CERT, was established in 1988 to deal with security issues on the Internet. It now partners with and supports the U.S. Department of Homeland Security's National Cyber Security Division and its US-CERT to coordinate response to security compromises, identify trends in intruder activity, identify solutions to security problems, and disseminate information to the broader community. CERT also conducts research and development to create solutions to security problems and provides training to help individuals build skills in dealing with cyber-security issues.