U.S. Department of Homeland Security
United States Secret Service

CERT
Software Engineering Institute
Carnegie Mellon

Insider Threat Study: Illicit Cyber Activity in the Government 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 range from a few lost staff hours to negative publicity and financial damage so extensive that a business may be forced to lay off employees or even 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 government sector. The report specifically focuses on employees who have perpetrated acts of financial fraud, document fraud, theft of intellectual property, and sabotage via computer against federal, state, and local government agencies. This effort is part of a larger research initiative, the Insider Threat Study, a collaborative endeavor of the United States Secret Service (Secret Service) National Threat Assessment Center (NTAC) and the CERT® Program of Carnegie Mellon University's Software Engineering Institute (CERT). 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 Insider Threat Study (ITS) is an exploration of employees who perpetrated acts of harm against an organization 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 government sector presents the fourth, and final, 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 Information Technology and Telecommunications Sector,* an examination of incidents within the IT sector, published in January 2008.

The cases examined in the ITS involve incidents perpetrated by current, former, or contract employees who intentionally exceeded or misused an authorized level of computer, system/network or data access in a manner that affected the organization. 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 Government Sector

This ITS report examines 36 incidents carried out by 38 insiders that occurred in the government sector between 1996 and 2002. Of the 36 incidents:

- 21 involved various types of fraud, to include 13 cases of financial fraud, 7 cases of document and/or ID fraud, and 1 case of computer fraud;
- 9 involved sabotage;
- 3 involved theft of confidential information; and,
- 3 involved both theft of confidential information and sabotage.

Key Findings

- The majority (58%) of insiders were current employees in administrative and support positions that required limited technical skills.

- Nearly half (43%) of insiders exhibited some inappropriate or concerning behavior prior to the incident.
- Financial gain was the motive (54%) for most insiders' illicit cyber activities.
- In over half the cases (56%), a specific event triggered, or was a contributing factor in, insiders' decisions to carry out the incidents.
- The majority (88%) of insiders planned their actions.
- Most (85%) of the insiders had authorized access at the time of their malicious activity.
- Access control gaps facilitated most (69%) of the insider incidents.
- Half (50%) of the insiders exploited weaknesses in established business processes or controls such as inadequate or poorly enforced policies and procedures for separation of duties (22%).
- Insiders were detected and identified by a combination of people (65%), processes (15%), and technologies (56%).
- In most (90%) cases, insiders faced criminal charges.
- Most (82%) insiders did not anticipate the consequences of their illicit activities.
- Insider actions affected federal, state, and local government agencies with the major impact to organizations being fraud resulting from damage to information or data (86%).

In addition, a small number of cases (19%) examined by ITS investigators involved the generation of fraudulent identification documents. Insiders carried out their illicit activities in these cases with little effort and for substantial financial gain. While few in number, these cases of document fraud represent a category of illicit insider cyber activity that could potentially have repercussions for the general public and to homeland security.

In the end, insiders jeopardized the public's trust in government agencies' abilities to protect citizens' personal and confidential information. Today, private sector interests are being subjected to increasing levels of scrutiny and requirements for public reporting. It is no less important – arguably more important – that government agencies pursue adequate safeguards for this data as well.

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. Suspected underreporting of insider incidents also makes it difficult to assess what percentage of all cases those uncovered by the ITS represent. Accordingly, this report and others from the ITS only report what was learned from known cases and avoid generalizing findings from cases examined to the unknown universe of all incidents or agency experiences in a given sector.

In addition, specific to the government sector, insider cases were not identified within all federal level agencies. To maintain the reliability of the methodology used for the study, if a federal agency had an insider case that was reported in the media and met the other criteria for the study then the case was included in this examination. Again, this may or may not be representative of the level of insider activity within the government.

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 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.