Insider Threat Study:

Illicit Cyber Activity in the Government Sector

Eileen Kowalski
Tara Conway
Susan Keverline, Ph.D.
Megan Williams
National Threat Assessment Center
United States Secret Service
Washington, DC

Dawn Cappelli
Bradford Willke
Andrew Moore
CERT® Program
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA

January 2008

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

CERT
Software Engineering Institute
Carnegie Mellon

TABLE OF CONTENTS

SECTION 1: INTRODUCTION[1]

Over an 18-month period, a government agency employee and two colleagues conspired to reduce or eliminate the bills of certain property and business owners in return for fees. As an agency customer service representative, the insider had limited authority to cancel bills for legitimate reasons. However, when a supervisor went on sick leave for an extended period the insider obtained and began using the supervisor's password and elevated access and authority to view and alter bills.

When the insider was promoted to a position in another department wherein he no longer had access to the billing computers, he enlisted a low-level colleague from his former department to help him continue the scheme. This colleague, who had limited authority to change bills, used a supervisor's unsecured computer while she was out of her office to access and alter accounts. A second colleague was brought into the scheme to recruit customers.

The insider used his profits from the scheme to purchase the apartment building in which he was living. The scheme eventually was detected when a quality check found 32 bill alterations above a certain level without explanations. Suspicion also was drawn to the insider after an office manager reported seeing the insider at a computer terminal when he wasn't supposed to be there. Loss from the scheme was estimated to exceed $3 million, almost all of which was recovered.

* * * * * * * *

A network administrator in a government agency arrived at work to find the network experiencing problems. He quickly diagnosed the problem and had the network up and running within half an hour. While working on the problem, he surreptitiously downloaded a <u>logic bomb</u> from the Internet and modified the network logs to make it appear as though his supervisor had sabotaged the network. After the insider produced the network log as evidence, the supervisor was placed on administrative leave, all the while protesting his innocence. The insider was only suspected after he started to exhibit odd behavior at work, and items stolen from the office were traced back to him. Investigation by an outside forensic specialist revealed that the logic bomb had been downloaded while the supervisor was away from the office, and that the logs were modified by the insider. The financial damage to the agency was not available at the time of this report.

Each of the incidents described above were committed by government sector "insiders," individuals who were, or previously had been, authorized to use the government agency information systems that they eventually exploited to perpetrate harm. As illustrated by these examples, government sector insiders have the potential to pose a substantial

---

[1] Parts of this document reflect guidelines from University of Chicago Press. The Chicago Manual of Style: The Essential Guide for Writers, Editors, and Publishers. 15th ed. The University of Chicago Press, Chicago.

threat by virtue of their knowledge of, and access to, employer systems and/or databases.

The Insider Threat to Critical Infrastructures

The insider threat is a problem faced by all industries and sectors today. It is an issue of growing concern as the consequences of insider incidents can include not only financial losses, but the loss of clients and business days. The actions of a single insider can cause damage to an organization ranging 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 organization to include disruption of operations or services critical to a specific sector, or the issuance of fraudulent identities that create serious risks to public safety and national security.

In *The National Strategy to Secure Cyberspace,*[2] the President's Critical Infrastructure Protection Board emphasizes the importance of continual evaluation to identify vulnerabilities in, and threats to, government and private information networks and systems. Specifically, the strategy emphasizes that it is the duty of all levels of government to secure their information systems to provide essential services. This plan also outlines the federal government's role in cyberspace security, specifying that it should look inward to ensure the safety of its own cyber infrastructure to provide continuity of government; and, that it is justified in some instances to take action external to the government to secure the protection of networks and systems critical to national security.

In addition, *The National Strategy to Secure Cyberspace* stresses the need to maintain functioning networks and systems that are interconnected between thirteen critical infrastructure sectors[3] comprised of public and private institutions:

- Banking and finance
- Information and telecommunications
- Transportation
- Postal and shipping
- Emergency services
- Continuity of government
- Public health
- Food
- Energy

---

[2] The National Strategy to Secure Cyberspace. (February 2003). http://www.whitehouse.gov/pcipb/
[3] Homeland Security Presidential Directive-7, issued in December 2003, contains an updated description of the critical infrastructure sectors. Specifically, Information technology and telecommunications are now designated as separate sectors. However, at the time this study was initiated the sectors were combined, and they are considered together for this report. See
http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

- Water
- Chemical industry and hazardous materials
- Agriculture
- Defense industrial base

As most of America's critical infrastructure is privately held, a key component of the strategy is the strengthening of public-private partnerships to secure the collective infrastructure and improve national cyber security. 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 specific initiative promotes awareness of the insider threat to organizations.

The Effort to Develop Information on the Insider Threat Issue

Efforts to identify prevalence of insider incidents

Estimates of how often government agencies and private companies are victimized by illicit cyber activity from within are difficult to make. It has been suggested that insider incidents are under-reported to law enforcement and prosecutors.[4] Reasons offered for such under-reporting include insufficient damage to warrant prosecution, insufficient evidence to prosecute, and concerns about negative publicity should reports of the incidents surface.[5]

Moreover, statistics vary regarding the prevalence of incidents perpetrated by insiders compared to those perpetrated by individuals external to the target organizations.[6] The E-Crime Watch Survey,™[7] carried out by the Secret Service, CERT, and *CSO Magazine* in summer 2006, elicited responses from 434 security and law enforcement executives on issues related to electronic crimes. Fifty-five percent of the organizations that were victims of electronic crime reported one or more insider incidents or intrusions, with 58% of the incidents known or suspected to have come from outsiders, 27% from insiders, and 15% of unknown origin.

Efforts to address the insider threat issue

Previous efforts focused largely on groups that could be conveniently sampled or represented more narrow areas of industry. These initiatives included workshops to

---

[4] National Research Council, Computer Science and Telecommunications Board, Summary of Discussions at a Planning Meeting on Cyber-Security and the Insider Threat to Classified Information, November 2000.
[5] CSO Magazine, United States Secret Service and CERT® Coordination Center. (2006). E-Crime Watch Survey. Framingham, MA: CXO Media [Hereafter referred to as 2006 E-Crime Watch Survey].
[6] Richardson, R. (2004). Ninth Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute [Hereafter referred to as CSI Survey]; Deloitte Touche Tohmatsu (2005). 2005 Global Security Survey; 2005 E-Crime Watch Survey.
[7] http://www.cert.org/archive/pdf/ecrimesurvey06.pdf

develop a foundation of knowledge on insider threats[8] and in-depth case studies of information technology (IT) insiders.[9] More recently, efforts aimed at addressing this issue have expanded to include

- annual surveys to identify the number of insider incidents experienced by organizations in a given year[10]
- workshops focused on mitigating the insider threat to the intelligence community[11]
- workshops to develop and test a framework for detection of insider activities that may pose threats to U.S. national security[12]

Individually, these initiatives have helped to expand the body of research and increase knowledge on this topic. However, gaps in the literature have made it difficult for organizations to develop a more comprehensive understanding of the insider threat. In particular, research to date has not examined the incidents from both behavioral and technical perspectives simultaneously. This lack of understanding has hampered efforts to address the issue from an approach that encompasses human resources, corporate security, and information security perspectives.

The Insider Threat Study (ITS) was initiated to take an in-depth look at reported insider incidents; specifically, the individuals who perpetrate these incidents and the types of incidents that have occurred within critical infrastructure sectors from both a behavioral and technical perspective. It is a collaborative initiative of the Secret Service National Threat Assessment Center (NTAC) and the CERT® Program of Carnegie Mellon University's Software Engineering Institute (CERT). The ITS was funded in part by the Department of Homeland Security, Office of Science and Technology.

---

[8] Anderson, R. H. (1999, August). Research and Development Initiatives Focused on Prevention, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems. Santa Monica, CA: RAND (CF151); Department of Defense (2000). DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team. Washington, DC.

[9] Shaw, E., Post, J., and Ruby, K. (August 31, 1999). Final Report: Insider Threats to Critical Information Systems: Typology of Perpetrators, Security Vulnerabilities, Recommendations.

[10] 2006 E-Crime Watch Survey; CSI Survey.

[11] Anderson, R. and Brackney, R. (2004). Understanding the Insider Threat: Proceedings of a March 2004 Workshop. http://www.rand.org/publications/CF/CF196/

[12] http://www.mitre.org/news/events/tech04/8.html

The Secret Service/CERT Collaboration

Since 2001, the Secret Service and CERT have collaborated in an array of efforts to identify, assess, and manage potential threats to, and vulnerabilities of, data and critical systems. This collaboration represents an effort to augment security and protective practices by
1. finding ways to identify, assess, and mitigate cyber security threats to data and critical systems that impact physical security or threaten the mission of the organization
2. finding ways to identify, assess, and manage individuals who may pose a threat to those data or critical systems
3. developing information and tools that can help private industry, government, and law enforcement identify cyber security issues that affect physical or operational security and assess potential threats to, and vulnerabilities in, data and critical systems

The ITS is a central component of this Secret Service/CERT multi-year collaboration. The ITS focuses in particular on the *people* who use or exceed their authorized access to information systems to perpetrate harm to organizations. The prevention of insider activity is important to the Secret Service because it can adversely affect the investigative and protective missions of the agency. Specifically, the Secret Service investigates

- violations of law related to financial crimes that include, but are not limited to, financial institution fraud, identity theft, access device fraud, and computer fraud
- computer-based attacks on our nation's financial, banking, and telecommunications infrastructure
- cyber security incidents, such as acts of sabotage, that cause the failure or compromise of information systems critical to the protective mission

The project draws from the Secret Service's expertise in behavioral and incident analysis and CERT's technical expertise in network systems survivability and security. Previous Secret Service studies have focused on identifying the thinking and behavior of subjects known to have posed a threat to public officials, public figures, and school children.[13] Information developed from these studies has proven to be operationally relevant in preventing future violent or disruptive incidents. The goal of this earlier research was to gather information to enhance threat assessment efforts – efforts to identify, assess, and manage the risk of harm an individual may pose before that individual has an opportunity to engage in violent, or disruptive, behavior.

---

[13] Fein, R. A., and Vossekuil, B. (January 2000). Protective Intelligence & Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials. U.S. Department of Justice. Vossekuil, B., Fein, R., Reddy, M., Borum, R., and Modzeleski, W. (June 2004). The Final Report and Findings of the Safe School Initiative: Implications For The Prevention of School Attacks in the United States. United States Secret Service and United States Department of Education.

Previous CERT research, sponsored by the U. S. Department of Defense (DoD), focused on cyber insider threats in the military services and defense agencies. That work effort is part of an ongoing partnership between CERT and the Defense Personnel Security Research Center (PERSEREC) undertaken in response to recommendations in the 2000 DoD Insider Threat Mitigation report.[14] The focus of that partnership is to identify characteristics of the environment surrounding insider cyber events evaluated for criminal prosecution by DoD investigative services. The primary use of this information will be to guide future operating, security, and personnel procedures to reduce the threat to critical information systems in the DoD and its contractor community. Since then, the CERT/PERSEREC partnership has been expanded to explore whether it is possible to develop predictive models of adverse insider behavior that consider technical deterrents as well as social, organizational, and psychological factors; and whether these models may apply to espionage as well as IT insider sabotage, both examples of trust betrayal.[15]

The Insider Threat Study

Initiated in 2002, the ITS is a multi-year exploration of employees who have 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, conducted from 2004 to 2007, to estimate the prevalence of insider activity experienced by a sample of public and private sector organizations[16]
- 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[17]
- an aggregate analysis of insider incidents across the critical infrastructure sectors where sabotage was the goal or intent[18]

---

[14] www.defenselink.mil/c3i/org/sio/iptreport4_26dbl.doc

[15] Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., and Trzeciak, R. F. (2006, December). Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis. Report available at http://www.cert.org/archive/pdf/06tr026.pdf

[16] CSO Magazine, United States Secret Service and CERT® Coordination Center. (2006). 2005 & 2004 E-Crime Watch Survey. Framingham, MA: CXO Media.

[17] Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., and Moore, A. (2004, August). Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. United States Secret Service and CERT Coordination Center. Report available at http://www.secretservice.gov or http://www.cert.org/archive/pdf/insidercross051105.pdf

[18] Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., and Rogers, S. (2005, May). Insider threat study: Computer sabotage in critical infrastructure sectors. United States Secret Service and CERT program. Report available at http://www.secretservice.gov

Reports from this study are written for a diverse audience that includes
- business executives and managers
- human resources personnel
- technical professionals
- security professionals
- law enforcement professionals
- legislators
- prosecutors

This report, *Insider Threat Study: Illicit Cyber Activity in the Government Sector*, presents the fourth, and final, series of findings from this multi-year research effort.

Study Purpose

The ITS research effort was undertaken to: 1) identify any pre-incident communications or behaviors exhibited by employees to include physical, social, and on-line behaviors; 2) identify vulnerabilities exploited by employees to carry out their illicit activities; and, 3) examine insider activity as it relates to critical infrastructure sectors.

Researchers examined insider activity within the critical infrastructure sectors for two primary reasons resulting from the perspective of prevention. Mainly, insider activity within the banking and finance, IT, and government sectors directly effects cases investigated by the Secret Service. Additionally, protecting the critical infrastructures was, and is, considered a national priority; yet, a comprehensive examination of insider activity within or across these sectors had not previously been addressed.

Research Questions

Several fundamental questions guided the ITS research:
1. Are there pre-incident behavioral or technical activities, plans, and communications that can be identified to inform how or why a person moves from the idea of targeting to the actual act of harm?
2. Are there investigative and protective implications of insider activity for the Secret Service?
3. What is the nature and impact of insider activity to specific critical infrastructure sectors?
4. Were there key life events or patterns in the histories of people who have perpetrated harm?
5. What are the technical details of how the insider conducted the incident?

Methodology

Only those cases meeting the study definition(s) that occurred in the United States between 1996 and 2002, in an organization that fell within a critical infrastructure sector, were included in this study.

Study Definitions

Defining "Insider"
The cases examined in the ITS are incidents perpetrated by insiders. Insiders are defined as current or former employees or contractors.

Defining "Illicit Activity"
For the purposes of the ITS, "illicit activity" is defined as cases where an insider intentionally exceeded or misused an authorized level of network, system, or data access; in a manner that affected the security of the organization's data, systems, or daily business operations.

Defining the Government Sector
For the purposes of the ITS, the government sector is defined as federal, state, and local government agencies, and private agencies contracted to serve as arms of the government or other private franchised organizations that provide services on behalf of the government.[19] Cases affecting contractor or franchised organizations that represent the government were categorized by the level of government that they serve.

Study Sample

A total of 149 cases across 12 of the 13 critical infrastructure sectors were identified through public reporting and searches of Secret Service case files. Public reporting included references in media outlets found through searches on Lexis-Nexis news and court databases and Internet searches.

Specific to the government sector, a total of 53 reported cases were identified. Seventeen cases were excluded through the course of the study where it was determined that: 1) the incident was not perpetrated by an insider; and/or 2) information was unavailable on the incident.

The government sector examined 36 incidents carried out by 38 insiders that occurred between 1996 and 2002. Of the 36 incidents
- 21 involved various types of fraud, to include 13 incidents of financial fraud, seven incidents of identity document fraud, and one incident of computer fraud[20]
- 9 involved sabotage
- 3 involved theft of confidential information
- 3 involved sabotage and theft of confidential information

---

[19] Term "State" also included "any state of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the trust territory of the Pacific Islands." Term "Local" also included "any county, city, village, town, district, or other political subdivision of any state, any Native American tribe or authorized tribal organization, or Alaska native village or organization, and includes any rural community or unincorporated town or village or any other public entity for which an application for assistance is made by a state or political subdivision, thereof." A description of the types and levels of government organizations examined in the ITS can be found in Appendix A of this report.
[20] "Financial fraud" refers to incidents of embezzlement; "identity documents" refers to social security cards, drivers' licenses, and other forms of identification accepted in the U.S. as official proof of identity and citizenship; and "computer fraud" refers to insiders charged with fraud utilizing a computer.

Organizations affected by insider activity in this sector included
- child and family support services/divisions
- motor vehicle registration department(s)
- police or other law enforcement department(s)
- judicial offices
- other assorted federal, state, city, and county offices and agencies

Research and Analysis
For each case examined in the study, researchers from the Secret Service and from CERT traced the insider incidents backwards in time from the initial point of harm to when the idea of committing the incident occurred to the insider. In retracing these incidents to their origins, researchers identified insider behaviors, communications, and activities – both online and offline – prior to and during execution of the incidents.

Researchers also reviewed primary source materials for each case, as available and applicable, that included police reports, federal law enforcement investigative reports, court records, mental health records, arrest records, accounts by third parties of the insider's history and behaviors, and secondary source material from news articles. Information gathered for each case included descriptive, demographic, behavioral, and historical data about each insider and facts about the insider's work history within the affected organization. Information gathered on the organization included demographic data, descriptions of the organization's policies, and technical security measures and specific damage suffered by the organization. Technical information gathered included details of how the incident was planned and carried out and technical activity to set up the incident.

This type of social and environmental information was not always included in the source materials collected. For that reason, ITS researchers conducted supplemental interviews, when possible, in an attempt to obtain information beyond these materials. Researchers attempted to conduct at least one supplemental interview per case. Interviews were conducted with case investigators, organization representatives, prosecutors, and a few insiders themselves. [21]

Researchers used the information gleaned from these sources to answer several hundred questions about the insider and the behavioral and technical aspects of the incident.[22] The questions were organized around the following major topic areas:
- components of the incident
- detection of the incident and identification of the insider
- pre-incident planning and communication
- nature of harm to the organization
- law enforcement and organizational response

---

[21] For this report, researchers interviewed representatives from at least 12 companies and at least 21 law enforcement or prosecutorial agencies.

[22] Information from the insider interviews was used to answer questions when corroborated.

- characteristics of the insider and the organization
- insider background and history
- insider technical expertise and interests

Specific examples of behavioral areas of inquiry included
- whether the insider had a plan to commit the harm
- the insider's motive for committing the incident
- whether the insider communicated any prior interest in harming the organization
- whether the insider displayed any concerning or noticeable behaviors prior to the incident
- whether the insider had a record of disciplinary actions at work
- whether the insider faced legal consequences

Specific examples of technical areas of inquiry included
- the insider's level of access at the time of the incident
- technical methods and tools used
- whether an account was compromised
- whether remote access was used
- which system logs were utilized to identify the insider
- the insider's level of experience with and interest in computers, hacking, programming, etc.

Questions pertaining specifically to the target organization included: descriptive information on the organization's methods of operations, structures, areas of business; and questions on policies regarding termination, acceptable use, and system back-ups.

Despite ITS researchers' best efforts, sources did not yield information to answer every question for all cases. For this reason, percentages in this report are based on the total number of cases for which information was available for a given research question.

In addition, some research questions in this study concern the insider (38 identified insiders), while others bear on the incident (36 identified incidents). Accordingly, the basis for analysis will vary depending upon whether the finding pertains to the insider or the incident.

Limitations

As noted previously, 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 the research team had access. Suspected underreporting of insider incidents also makes it difficult to assess what percentage of all cases are represented in the ITS. Accordingly, this report and others from the study will present only what was found among the known cases. This limits the ability to generalize the study findings to all organization experiences in a given sector and underscores the difficulty other researchers have faced in trying to better understand the insider threat.

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 insight into actual criminal and other illicit acts committed by insiders. This insight may be useful to those individuals employed in critical infrastructure sectors who are charged with protecting <u>critical assets</u> as they begin to examine ways of improving their defenses against insider threats.

Organization of the Report

The remainder of this report is organized into three sections. Section 2 presents the findings of the study. Section 3 discusses the implications of those key findings. Section 4 presents the conclusion, which highlights the major findings and potential implications of illicit insider activity in the government sector.

Finally, this report includes four appendices. Appendix A provides tables containing information on the size and type of the agencies affected; the states where the agencies were headquartered; the financial damage to the affected agencies; and information on the insiders. Appendix B contains synopses of additional case examples that are illustrative of incidents examined for this study. Appendix C contains a glossary of technical terms used in this report. The first use of each term included in the glossary is indicated in the text of the report with an underscore. Appendix D identifies and acknowledges the efforts of individuals who worked on this project.

SECTION 2: FINDINGS OF THE INSIDER THREAT STUDY OF ILLICIT CYBER ACTIVITY IN THE GOVERNMENT SECTOR

The ITS government sector findings are presented in this section under four headings:
- The Insiders
- The Incidents
- Detecting the Incidents
- Consequences of the Incidents

The Insiders reports findings related to the characteristics of the individuals who perpetrated the incidents, their roles within the target organizations, their workplace behaviors, and their motives for carrying out their illicit activities. Information provided under *The Incidents* concerns the insiders' pre-incident planning and technical information regarding methods for advancing the incidents. *Detecting the Incidents* presents findings concerning the manner in which the insiders' illicit activities were uncovered and the insiders were identified. The final section, *Consequences of the Incidents*, is comprised of two subcategories. The first subcategory reports findings related to insiders' perceptions of the potential consequences of their actions, disciplinary actions taken by the target organizations, charges filed, and the outcome of cases. The second subcategory describes the characteristics of the target organizations and the damages they incurred.

Thirty-six incidents and 38 insiders were examined within the ITS government sector. As noted, some research questions in this study concern the insider, while others bear on the incident. Accordingly, the denominator for statistics in this report will vary depending upon whether the finding pertains to the insider or the incident.

The Insiders

Characteristics

Findings
- Insiders did not share common demographic characteristics.
- The majority of insiders were current employees in administrative and support positions that required limited technical skills.

Supporting Data
Insiders did not share a common demographic profile.
- There were an equal number of men (50%) and women (50%).[23]
- The insiders were primarily African American (42%) and Caucasian (39%). A minority were Asian (8%) and Hispanic (5%).
- Insiders' ages ranged from 19 to 55.[24]

---

[23] Table # 1 in Appendix A.
[24] Table # 2 in Appendix A.

- Nearly half (48%) of the insiders were married and the other half were either single/not married, divorced, and/or separated.
- Just under one third (32%) of the insiders were living with their spouses, significant others, and/or children at the time of the incidents.
- Under one third (31%) of the insiders had prior arrest histories for financial/fraud-related offenses (14%), non-financial/fraud-related theft offenses (6%), alcohol or other drug-related offenses (3%), violent offenses (3%), and other offenses (3%).

Insiders were largely employed in administrative and support positions.
- Most (58%) of the insiders worked in administrative and support positions, as data entry clerks, typists, customer service representatives, and bookkeepers.
- Half of the insiders who worked in these administrative and support positions had been assigned supervisory or leadership roles.
- A quarter (26%) of the insiders worked in positions, such as system administrator, programmer, or IT specialist that required technical skills.

Nearly all of the insiders were current employees of the target organizations.
- Most of the insiders (90%) were current employees, were working full time schedules (78%) with authorized access to the organizations' systems and networks (85%) at the time of the initial damage.
- Sixteen percent of the employees were contractors, sub-contractors, or temporary workers at the time of the incident.
- Insiders' work assignments involved varying levels of supervision and interaction with other employees. Some insiders functioned independently, while others functioned as members of teams for which 37% served as team leaders. The nature of most insiders' work required minimal supervision (78%), and most of the insiders had just one supervisor (77%).

Workplace Behaviors

Finding
- Nearly half of the insiders exhibited some inappropriate or concerning behavior prior to the incident, but had no recorded incidents of violating organizational policies.

Supporting Data
In almost half the cases (43%), the insiders exhibited inappropriate behavior that was noticed by others prior to the incident. Of those insiders:
- Many came to the attention of their supervisors (71%) and coworkers (57%) for behavior such as calling in sick frequently; leaving work early; demonstrating a poor attitude; and engaging in heated arguments with colleagues in the workplace.
- Others came to the attention of law enforcement (7%), a subordinate (7%), or a family member (7%) as a result of exhibiting some type of concerning behavior.

Eighty-four percent of the insiders had no recorded incidents of violating organization policies.

In the majority of cases (79%), there were no indications that the insiders were perceived by others as disgruntled employees.

Motives

> *A state motor vehicles department (DMV) employee engaged in a conspiracy to help motorists obtain drivers' licenses illegally. The insider initiated the fraudulent activity at the request of a friend who asked for the insider's help in securing a driver's license for her son who did not meet requirements for a driver's license. The insider agreed to produce the license in exchange for a fee. The insider and her accomplice then began recruiting "customers" for their illegal activities. The accomplice would solicit customers, many of whom were immigrants, and direct them to the insider's counter at the DMV branch office. For each license produced, the insider would falsely record that the applicant had surrendered a valid driver's license from another state when in fact no such transaction had occurred.*

Findings
- Financial gain was both the motive for, and objective of, most insiders' illicit cyber activities.
- In over half the cases, a specific event triggered, or was a contributing factor in, the insiders' decisions to carry out their activities.

Supporting Data
Motives and Objectives
Over half of the insiders (54%) were motivated by financial gain.[25] All insiders whose motives were financial gain committed fraud.

Insiders were also motivated by revenge (24%). Those insiders motivated by revenge committed harm to the target organization which included
- incidents of sabotage (67%)
- incidents of theft of confidential information (11%)[26]
- incidents involving both theft of confidential information and sabotage (22%)

Finally, some insiders were motivated by a specific grievance (14%). Some insiders (21%) communicated negative feelings or grievances toward the target organizations. Most of these communications were verbal:

---

[25] For each insider, researchers coded both the insider's motive (the reason or reasons why the insider engaged in the incident; for example, revenge) and the insider's goal (what the insider was trying to accomplish with the incident; for example, destroying the company's reputation).
[26] Information available on only 35 cases and insiders.

- 71% of these insiders communicated negative feelings about the targets to others.
- 29% of these insiders communicated negative feelings about the targets to the targets themselves.

Few insiders communicated a direct threat of harm (9%) to the target organizations.

In approximately half the cases (51%), financial gain was the insiders' primary goal or objective for carrying out their activities. Insiders also sought to sabotage information data/files (16%); sabotage the information systems/networks (14%); steal intellectual property (11%); and help others (11%), such as described in the case example provided above.[27]

Triggers and Contributing Factors
In over half the cases (56%), a specific event triggered, or contributed to triggering, insiders' illicit activities. These events included impending or actual employment-related termination or demotion; transfer or other disciplinary action (40%); financial hardship or bribe (40%); a personal problem unrelated to the organization (15%); a dispute or dissatisfaction with management, the organization, or its policies (10%); or another event (5%).[28]

In over half the cases (67%), the insiders had communications with others that may have triggered their actions. Of these cases
- In 37%, insiders received direct or indirect encouragement from others to perform the illicit activity.
- In 36% of the cases, general communications may have influenced the insiders' actions.
- In 27% of the cases, others provided the insider information in furtherance of the incidents.

Insiders' access to personal data may have been a contributing factor. In many incidents (56%), insiders used authorized access to alter or obtain an individual's personal data in some manner.[29] Of these incidents
- 90% involved insiders who altered or obtained an individual's personal data to profit or benefit financially. For example, insiders' accessed or altered personal data to
    - generate false documents or counterfeit personal identifiers, to include false dates of birth and social security numbers, for payment (39%)
    - remove fines, reduce bills, or delete negative information for payment (33%)
    - increase or create benefit accounts to include retirement, disability, and social service benefits for themselves, friends, or family members (28%)

---

[27] Multiple responses possible; total may be over 100%.
[28] Multiple responses possible; total may be over 100%.
[29] These percentages are based on the number of incidents (36).

- 10% involved insiders who altered or obtained an individual's personal data for revenge or to help others.

Prior to their actions, a number of insiders (41%) experienced a major life change or loss. Of these insiders, 75% had experienced difficulty in coping with the major change or loss.

The Incidents

Pre-incident Planning

> *Employees at a motor vehicle department branch office generated fraudulent drivers' licenses for immigrants who did not have the required forms of identification to obtain licenses legally. The fraudulent licenses were used to establish lines of credit at local car dealerships and furniture stores that the insiders then defrauded of $250,000.*
>
> *Pre-authorized forms created a vulnerability in the office's procedures for verifying that applicants possessed valid forms of identification. One of the employees involved exploited this loophole to have the falsified paperwork pre-approved. This employee then used her knowledge of the electronic steps required in generating a license to complete the process. She abused her access to the computer system by making online transactions that were outside of her job responsibilities. The employee and her accomplices received $250-$500 per false license generated.*

Findings
- The majority of insiders planned their actions.
- Others were aware of, involved in, or benefited from insiders' illicit activities.

Supporting Data
In the vast majority of cases (88%), insiders developed plans prior to carrying out their illicit activities. In 94% of the cases insiders conceptualized the idea prior to the initial illicit activities. In a little more than one-third of the cases (36%), insiders engaged in some type of preparatory behaviors. Preparatory or planning activity included
- repeatedly attempting to access the system
- discussing with others details of how to carry out their activities
- emailing configuration, commands, and/or login passwords from work to home
- partially modifying records to test the system
- granting him/herself access to systems

The majority (60%) of insiders engaged in preparatory or planning activities that were noticeable to others:
- 45% of these behaviors occurred offline.
- 35% occurred online.

- 20% occurred both online and offline.

The majority (92%) of preparatory behaviors did not affect the organizations' daily business operations, reputations, facilities, or personnel.

In most incidents (58%), others – in some instances co-workers – had information about the insiders' plans, intentions, and/or activities. Some individuals were involved in the planning, while others were aware of the insiders' plans or intentions, but not actually involved in the planning.

In most cases, the insiders acted alone in carrying out the illicit activities. However, 36% of the cases involved collusion with others to carry out the incidents. Thirty-one percent of the cases involved collusion with others *prior* to the incidents. One-third of the cases in which the insider carried out his or her illicit activity in collusion with other individuals involved foreign nationals. In most of the cases the co-conspirators benefited from the activities.

The accomplices' affiliations with target organizations varied; some were associated with the affected organizations and others had no affiliation with the target organizations. In the cases in which others were involved, nearly 20% were present with the insiders during the incidents.

Technical Details of the Incidents

> *A police communications officer conspired with a member of a criminal organization to create over 195 drivers' licenses over a two-year period for individuals who were unable to obtain licenses legally. The insider, who was responsible for running driver's license checks for police officers in the field, began her activity by looking up information in return for money from an outside contact. However, she came to realize that she not only had access to read the data, but also was able to modify it. As a result, she exploited her excessive access to the agency database to create new licenses for her co-conspirator in return for money.*

Findings
- Most of the insiders had authorized access at the time of their malicious activities.
- Access control gaps facilitated most of the insider incidents.
- Most insiders modified or deleted information using only user commands.
- Some insiders used technical means for compromising accounts or carrying out their malicious activities.

Supporting Data
The majority of insider activity (69%) was facilitated because of access control issues. For example

- Access exceeded what was needed to do the job.
- Access was obtained following termination or changes in position.
- The insider was able to use another employee's account or computer.
- Sufficient technical controls were not in place.
- Technical insiders were able to circumvent technical controls.

Eighty-five percent of the insiders had authorized access to the target organizations' systems or networks when they committed their illicit activities. Of these
- 50% were authorized, unprivileged users.
- 24% were authorized, privileged users.
- 12% had system administrator access.

When hired
- 7% were granted restricted access.
- 60% were granted authorized, unprivileged access.
- 17% were granted authorized, privileged access.
- 17% were granted system administrator access.

In 42% of incidents, insiders used an account other than their own in carrying out their malicious activities. Over half of the insiders (58%) were able to commit their activities using only their own usernames and passwords. Thirty-five percent compromised someone else's account, including
- a system administrator account
- expired accounts
- other employees' accounts
- an account at the insider's previous employer after leaving for a new job
- another employee's computer left logged in without a screen lock
- a shared account

Insiders used a variety of non-technical methods to compromise accounts, including the following:
- coerced or intimidated coworkers or subordinates into revealing their passwords
- used accounts of employees who shared their passwords among the group
- kept organization's laptop after resignation
- used coworker's computer that was left logged in without a screen lock

Insiders also employed different technical methods to compromise accounts, including the following:
- used a password cracker
- modified the program used by employees to change their passwords so it saved their new passwords in a file[30]
- accessed system administrator account using an unpatched system vulnerability

---

[30] This insider did not actually use those passwords to compromise accounts, however, due to the extreme vulnerability it poses and its obvious malicious intent, we chose to include the description here.

- changed passwords for other employees' accounts
- used "wide open sudo"[31] to perform system administrator commands
- used a system administrator account to add privileges to the insider's personal account, then changed the privileges on some files to the same privileges so that the insider now had access to them

In addition, system administrator access was misused by several insiders in a variety of ways, including

- downloaded a logic bomb from the Internet, then manipulated the log file entries to tie the actions to the insider's supervisor's account
- made unauthorized, covert modifications to the source code for the production system and released it into production
- inserted a logic bomb into an "out of the box" system script
- modified the insider's supervisor's .profile[32] to execute a logic bomb
- modified system logs to remove all signs of the insider's actions

Eleven percent of the insiders used backdoors.[33] Eighteen percent of the insiders used remote access. Few insiders (5%) used social engineering to assist them in gaining access to the information systems/networks.

Most insiders (89%) modified or deleted information. Eighty percent of insiders used only user commands for their actions, but 28% of the incidents were technically sophisticated, using a script or program, technical actions to set up the incident, or creating an unauthorized account. Fourteen percent of the incidents involved use of a malicious script or program.

Business Process Issues Related to the Incidents

Two claims representatives at a government agency engaged in a scheme with the boyfriend of one of the insiders and his accomplice. As a result, official U.S. identity documents were generated for 151 illegal aliens and credit card fraud was committed with losses in excess of $43,500. The insiders were paid $200 for each illegal identity document, and $50 for each report they generated of personal data to be used for credit card fraud. The scheme was facilitated by design flaws and lack of technical controls in the agency's business processes.

When processing an application for a new identity document, the employees were required to manually look up the applicant in another government agency's database to validate the applicant's identity, and to verify that the applicant met

---

[31] *sudo* is a UNIX command that allows users to run programs with the security privileges of another user (normally the system's superuser). See http://en.wikipedia.org/wiki/Sudo for more information.
[32] In the UNIX operating system, the .profile file contains commands that are executed when the user logs into the system.
[33] Some insiders used their own accounts as well as another account or method to commit their malicious activities.

the criteria for obtaining the identity document. However, the business processes of the two agencies were not designed to work together, and in cases where applicants went directly from the first agency to the second on the same day, the data was not necessarily entered yet into the original agency's database. Therefore, technical business rules were missing for enforcing data integrity and data integrity was not enforced via the manual process.

Findings
- Some insiders exploited weaknesses in established business processes or controls such as inadequate or poorly enforced policies and procedures for <u>separation of duties</u>.[34]

Supporting Data
Half of the insiders exploited vulnerabilities in business processes.[35] For example
- Insiders were able to circumvent subtle flaws in business processes, or processes that lacked technical controls for enforcement.
- Insiders were able to circumvent technically enforced business processes due to improper <u>access controls</u>, via collusion among multiple insiders, or using social engineering.
- Technical insiders exploited vulnerabilities in technical policies and procedures.

Almost a quarter (22%) of the incidents involved violations of separation of duties. Seventeen percent of insiders exploited vulnerabilities in security controls that should have prevented these violations. For example
- Poor implementation of <u>role-based access control</u> provided some insiders with means of overriding separation of duties.[36]
- One insider easily circumvented separation of duties because they were implemented via policy rather than enforced through technical controls.
- One insider (3%) was able to circumvent separation of duties using his elevated system access rights.
- In several incidents, insiders with different roles colluded to carry out their scheme.
- Account compromise enabled one insider to perform multiple roles in the system.

---

[34] Separation of duties is the process of disseminating the tasks and associated privileges for a specific business process among multiple users in order to prevent fraud and errors.

[35] A collection of related, structured activities—a chain of events—that an organization defines to achieve a business goal. Typical business processes include receiving orders, selling, delivering, and distributing products, invoicing for services, and accounting for money received. A business process usually depends upon several functions for support, e.g., IT, personnel, and accounting.

[36] Role-based access control restricts system functions to authorized roles, rather than individual users. Within a system, roles are created for various job functions. The permission to perform certain operations in the system is assigned to specific roles. Each system user is then assigned a particular role or roles, and through those role assignments acquire the permissions to perform particular system functions.

Detecting the Incidents

> *An insider within a lottery agency claimed 126 winning lottery tickets worth $63,000 over a period of a year and a half. A convenience store manager finally became suspicious when he noticed that a number of the winning lottery tickets redeemed were all badly mangled. The prize codes and sight validation codes on the tickets were not readable, necessitating that the manager use the lottery's computer program to validate them. He turned the tickets into the lottery's district manager who had also received mangled winning tickets from two other store managers. At first lottery officials verified that the tickets were indeed winners using the same computer program. However, when they reconciled the tickets against an archive of winning ticket data (from tape backup) they found that the tickets were not marked as winners in the original system data. Through established <u>configuration management</u> and backup processes, evidence was collected and the insider was successfully prosecuted for the fraud.*

Finding
- Insiders were detected and identified by a combination of people, processes, and technologies.

Supporting data
Most (65%) of the incidents were detected by non-technical means. Over half of all incidents (56%) were detected by irregularities in software or systems, and 15% of all incidents were detected by system failure. Eleven percent of all incidents were detected when the insiders' actions caused system activity to be denied abnormally.

Incidents were initially detected by technical and security personnel, law enforcement and other investigators, non-technical management and staff, and external informants or victims.[37]
- Some incidents were detected and the insiders identified by individuals whose primary job function or role was security-related: system administrators (15%), IT security (9%), other security personnel (15%), and/or law enforcement (12%). Insiders were identified by: system administrators (17%), IT security (25%), other security personnel (22%), and/or law enforcement (61%).
- Some insiders' activities were detected by employees whose formal job function or role was not in system or security management: company non-security personnel (26%), supervisors (24%), or the person responsible for the system (3%). Insiders were identified by: company non-security personnel (31%), supervisors (31%), or the person responsible for the system (6%).
- Some incidents were detected by individuals outside the target organizations who were not in law enforcement: customers (15%) and victims (6%). In addition, external informants identified the insiders in 11% of the incidents.
- In 11% of the detected incidents, the insider turned him or herself in.

---

[37] Many insiders were detected by more than one person.

In 94% of the incidents, insiders were identified using one or more manual procedures such as internal audits (21%), phone records (9%), self-reporting (15%), and association of their illicit actions with their user names (32%) or source IP addresses (12%).

Fifty-six percent of the insiders were identified by forensic exams of the targeted organizations', networks, data, or systems; 21% by forensic exams of the insiders' home equipment; and 35% by forensic exam of insiders' work computers.

In 82% of the incidents, one or more system logs were used to identify or corroborate the identity of the insiders.[38] Of these incidents
- 67% of those incidents made use of available database or application logs.
- 17% used remote access logs.
- 17% used file access logs.
- 17% used logs of file changes.
- Three other types of logs were used for single incidents: FTP logs, audit logs to trace machine of access, and DNS logs.

Over half of the insiders (60%) were aware of the technical security measures that were employed by the organization.

Half of the insiders took technical actions to conceal their identities, actions, or to mitigate possible negative consequences.
- Insiders mainly (57%) used technology to delete or modify records of the incidents.
- Other insiders (24%) actively raised suspicion in the direction of others and denied their part in the incidents when confronted.

These methods of concealment included
- used others' computers or accounts, including backdoor accounts and system administrator accounts
- reformatted a hard disk on his laptop
- deleted files, including a modem access log and system history files
- modified system logs to frame supervisor
- wrote malicious code that deleted itself after execution
- modified production code to eliminate automatic email sent to security when data was modified
- asked a subordinate to erase all backup tapes, then go offsite to obtain the additional backup tapes
- sent a letter to someone explaining the insider's plan for exposing security problems and back dated it by a year

---

[38] Many insiders were identified using more than one type of system log.

Insiders primarily (79%) carried out their actions in the workplace during normal working hours; most (82%) initiated actions while at their employment facilities versus using remote access from home (18%). None of the insiders carried out their actions both remotely and at work.

Consequences of Incidents

For Insiders

> *A federal claims representative decided to take revenge when he was banned from an online chat room following a "cyberspace altercation" with the chat room administrator. Using a co-worker's computer, the insider listed the chat room administrator as deceased in the federal government database which he used for his job. The action was detected when the victim attempted to open a bank account and the bank informed her that she was listed as deceased in the official federal database. Suspicion immediately fell upon the co-worker whose computer the insider had used in committing his attack. However, while chatting online prior to the incident, the insider told a third party that he had the ability to list someone as deceased in his employer's computer system. He also had posted an online threat against the victim in a chat room, along with a picture of himself. Those two chat sessions were used to identify him as the perpetrator. Following his exposure as the perpetrator of the insider attack, the claims representative asserted that he did not realize the seriousness of what he had done and that he only hoped to inconvenience the chat room administrator. He was sentenced to one year probation and ordered to pay restitution in the amount of $700.*

Findings
- Insiders faced criminal charges in most cases.
- Insiders did not anticipate the severity of the consequences for their illicit activities.

Supporting Data
Insiders faced criminal charges in most of the cases (90%). Charges were brought under state laws (53%) or federal laws (44%).[39]

Of those cases where an insider was charged criminally, most insiders (74%) plead guilty.
- A small percentage went to trial and were found guilty (9%), plead *nolo contendere* (6%), or the case was dismissed (6%).
- Two cases (6%) were still pending judicial outcome at the completion of this study.
- Cases were not usually appealed (75%).

---

[39] Table # 3 in Appendix A.

- In 32% of the cases others were charged. The majority of these charges were for conspiracy.

In over half the cases (53%), the insider faced some length of incarceration.
- In most cases (68%) the insider was given probation or placed under supervised release.
- Often punishment also included restitution in various amounts (56%).

Other judicial outcomes included, community service (15%), fines (6%), or no sentence was given (9%).

At the time the study was conducted, most insiders (53%) were unconfined and completely unmonitored. Several others (22%) were still on probation. The remaining few had been released on bail (6%), were on parole (9%), or were still incarcerated (6%).

In 76% of the cases examined, disciplinary actions were taken within the organizations in response to the insiders' acts.
- Most insiders (57%) were terminated from their positions within the target organizations.
- In 40% of the cases the insiders resigned at the time of investigation.
- In 11% of the cases, the insiders did not lose their jobs, but were demoted.

Most insiders (82%) claimed not to have thought about possible negative consequences of their illicit activities.

For Target Organizations

Over a two-year period, a government agency claims examiner falsely approved payments of disability claims. The financial loss to the agency was in excess of $600,000. The insider carried out her illicit activities by exploiting privileges that she had retained from a previous position in another agency division that allowed her to access already established claims. She then used her legitimate authority to act on established claims to approve the fraudulent payments. The insider's actions were uncovered when a third party who did not work for the agency reported suspicions concerning the insider's actions to agency authorities.

Findings
- Insider actions affected federal, state, and local government agencies.
- The major impact to organizations was financial loss resulting from damage to information or data.
- Most agencies had established technical security measures in place and processes for responding to illicit activity.

Supporting Data

Organization Characteristics

ITS government sector target organizations included agencies and departments at all three levels of government – federal, state, and local. These organizations varied in size, field or discipline, and functions.

- The incidents of insider harm were divided almost equally among the three levels of government, with 39% of the incidents involving local agencies, 31% state agencies, and 31% federal agencies.[40]
- The agencies varied in size. Thirty-six percent were classified as small (1-500 employees); 29% as medium-sized (501-10,000); and 36% as large (over 10,000 employees) agencies. [41]
- Most of the federal agencies included in the study were large organizations with over 10,000 employees, whereas the state agencies tended to be smaller in size with less than 10,000 employees.
- The majority of the local agencies had 500 or fewer employees; with the exception of one local agency that had over 50,000 employees.

The government organizations targeted for insider acts also varied by discipline, field, and functions and included law enforcement, social services, motor vehicle administration, judicial services, lottery, and environmental protection.

- Half of the organizations (50%) maintained a headquarters and five or more satellite offices.
- Nearly all (83%) conducted operations exclusively in the United States.
- Nearly all (94%) were considered stable at the time of the initial damage with no imminent layoffs.
- Over half of the organizations (61%) conducted business online.
- Over half (53%) handled classified government information as part of standard operations.

In the majority of incidents, the target government agency was the victim of only one incident of insider harm. However, 8% of these government agencies experienced multiple incidents of insider harm reported in this study; one federal agency was affected three times, in several different states; and both a state level agency and a local government agency were the victims of two incidents each. Government agencies in Florida and Texas experienced the greatest number of incidents.[42] The most reported incidents occurred in 1997 and the least in 2002.[43]

Impact to Organizations

The types of harm incurred by government sector target organizations included

- financial fraud (36%)
- identity document fraud (19%)

---

[40] Table # 4 in Appendix A.
[41] Table # 5 in Appendix A.
[42] Table # 6 in Appendix A.
[43] Table # 7 in Appendix A.

- computer fraud (3%)
- sabotage (25%)
- theft of confidential information (8%)
- a combination of sabotage and theft of confidential information (8%)

In most of the incidents, insider incidents damaged target organizations' information or data files.
- Insiders successfully altered, inserted, or deleted information or data files in 86% of these incidents.
- The integrity of the information/data was affected in the majority (72%) of the incidents.
- Insiders' actions resulted in corruption of information in 75% of the incidents.
- In 77% of the incidents, business operations were not affected by the insiders' activities. In seven incidents where business operations were affected, two incidents affected operations for greater than 15 days and in five incidents business operations were affected between 1-15 days.

The majority (69%) of government organizations experienced some degree of financial damage.[44] Of these
- 38% resulted in less than $20,000 worth of damage.
- 21% caused between $20,000 and $50,000 in damage.
- 17% caused between $50,000 and $100,000 in damage.
- 17% caused between $100,000 and $300,000 in damage.
- Only 8% caused over $300,000 in damage to include one insider who caused $3,000,000 worth of damage.

Organization Practices and Responses
Most of the organizations recognized the importance of technical security measures.
- Three-quarters (72%) of the organizations had policies on acceptable use.
- Employees in over half (64%) of the organizations were informed of organizational policies regarding acceptable use through awareness programs.
- The majority (64%) of the organizations had the ability to monitor for IT violations by either maintaining an intrusion detection system or by conducting internal audits.
- When violations were detected, organizations typically responded with demotion (67%), verbal warning or counseling (44%), written warning (22%), involuntary transfer or dismissal (22%), and suspension with/without pay (11%).
- Only one (5%) organization reinforced its policies, practices, and technology with cyber insurance.

The government agencies successfully recovered the information in most (83%) instances.

---

[44] Table # 8 in Appendix A.

- None of the government agencies sought external assistance to recover from the damage.
- In one incident (3%) the government agency only partially recovered the lost information.
- In a few incidents (9%), the government agencies were unable to recover the information at all.

Organizations contacted law enforcement in almost all incidents (92%).[45]
- Federal law enforcement agencies were notified most frequently (33%).
- Local law enforcement was notified 30% of the time.
- State law enforcement was notified 20% of the time.
- In 17% of the incidents multiple law enforcement agencies were notified.

Other Consequences

> *A supervisor in a federal agency conspired with three foreign nationals who were not government employees to assist immigrants seeking residency in the U.S. in return for bribes totaling approximately $50,000 over a two-year period. The immigrants' applications had either been previously denied or referred for a court hearing after being submitted and reviewed through official channels. Using his authorized system access but circumventing standard business processes for this organization, the insider changed the information and approved the applications of almost fifty applicants who would otherwise have not met the criteria to remain in the U.S.*

Finding
- A minority of cases had a noticeable impact on the general public and demonstrated the potential for risks to homeland security.

Supporting Data
- As noted earlier in the report, thirteen percent of the insiders in the government sector cases colluded with foreign nationals.

- Seven cases (19%) involved document fraud and one case (3%) involved the release of personal information that resulted in the following notable consequences:
  - o Over 200 illegitimate federal identity documents were issued to illegal aliens, permitting them to work and live in the U.S; some were granted asylum when they had been marked for deportation.
  - o Over 1300 fraudulent state driver's licenses were issued. A majority of these were issued to illegal aliens. Some of the licenses displayed the social security numbers of other, legitimate license holders.

---

[45] Table # 9 in Appendix A.

- Nearly $300,000 in credit card fraud was committed as a result of falsely issued federal and state identity documents. In addition, 2500 queries of personal and confidential information run by one insider were eventually tied to an unknown amount of credit card fraud.
- Improper disclosure of personal and confidential information by one insider resulted in a murder.

SECTION 3: IMPLICATIONS OF THE KEY FINDINGS FOR THE PREVENTION OF ILLICIT INSIDER CYBER ACTIVITY IN THE GOVERNMENT SECTOR

This section addresses implications of the key findings for the government sector to develop strategies for preventing insider incidents. The discussion of implications is organized under six categories: *The Insiders*, *The Incidents*, *Detecting the Incidents*, and *Consequences of the Incidents*. The relevant findings for each category are repeated in this section. The findings are followed by a brief description of the implications and commentary that describes the implications in greater detail.

The Insiders

Key Findings
Characteristics
- The majority of insiders were employed in administrative and support positions that required limited technical skills.

Workplace Behavior
- Nearly half of the insiders exhibited some inappropriate or concerning behavior prior to the incidents, but had no recorded incidents of violating organizational policies.

Motive
- Financial gain was both the motive for, and objective of, most insiders' illicit cyber activities.
- In over half the cases, a specific event triggered, or was a contributing factor in, insiders' decisions to carry out their activities.

Implications

- Organizations cannot assume that technically skilled IT professionals are more likely to engage in illicit activity than other insiders.

- Organizations should train supervisors to recognize, document, and respond to inappropriate/concerning behavior in the workplace.

- The market value of information contained in government databases, in particular, identity-related data, may increase the risk of illicit cyber activity to obtain and sell this information for personal financial gain.

Organizations cannot assume that technically skilled IT professionals are more likely to engage in illicit activity than other insiders. Earlier works concerning illicit insider activity[46] expressed concern that these perpetrators would be technically skilled

---

[46] Shaw, E., Post, J., and Ruby, K. (August 31, 1999). Final Report: Insider Threats to Critical Information Systems: Typology of Perpetrators, Security Vulnerabilities, Recommendations.

IT professionals working as systems administrators, programmers, and network administrators. These insiders, therefore, would be able to carry out complex attacks and cause serious harm. However, ITS researchers found that the majority of the insiders in the 36 incidents examined for the government sector report held administrative and support positions that required limited technical skills. This finding suggests that assessments of the risk of employee insider activity should not be centered on position or skill levels alone; a finding also reflected in later insider threat research,[47] which concluded that technical skill was not a characteristic of the most frequent attackers.

Organizations should train supervisors to recognize, document, and respond to inappropriate/concerning behavior in the workplace.
Organizations should not assume that insider activity within this sector will be conducted by employees with histories of policy violations and disciplinary problems. Most ITS government sector insiders were not considered problem employees. They did not have histories of disciplinary actions or recorded violations of organizational policies. However, many exhibited a range of inappropriate behavior such as truancy, tardiness, excessive sick days, and unaccounted absences during the work day. The findings suggest that the insiders were more likely to exhibit less serious, but concerning behavior that was noticeable to others prior to the incidents. While only 43% of the insiders exhibited inappropriate or concerning behavior prior to the incident, in almost half of these cases, the behaviors could have alerted organization officials to the need to initiate closer monitoring of these employees.

Many times, less serious types of behavior are noticed in the workplace, but are not documented because they do not rise to the level of a policy violation. For example, an insider was counseled for inappropriate actions and comments shortly after being hired as a system administrator. The insider subsequently developed a pattern of arriving late for work, disappearing during the work day for extended periods of time, and leaving early. When confronted by his supervisor, the insider became hostile and was warned that if his behavior continued, he would be dismissed. The insider ultimately exceeded his access, installed a <u>logic bomb</u> on the system, and framed his supervisor for his actions.

Inappropriate behaviors such as those described in the above case example, may be early warning signs of insider activity. Organizations should encourage supervisors to recognize and document such behavior and begin monitoring, where permissible, employee activity accordingly. This may enable an organization to intervene before an employee is able to carry out illicit activity.

---

[47] Shaw, E. D. and Fischer, L. "Ten Tales of Betrayal: An Analysis of Attacks on Corporate Infrastructure by Information Technology Insiders," Report 1—Overview and General Observations, *Technical Report 05-13* (FOUO). Monterrey, CA.: Defense Personnel Security Research Center, 2005.

The market value of information contained in government databases, especially identity-related data, may increase the risk of illicit cyber activity to obtain and sell this information for personal financial gain. Financial gain was the predominant motive and objective for incidents examined in the government sector report. Much of the damage to data and systems inflicted in this sector occurred in pursuit of a financial goal rather than with malicious intent to harm the organization, the system, or affiliated employees. In the majority of these incidents, insiders modified, viewed, or obtained sensitive data in exchange for monetary compensation from individuals both internal and external to the organization.

Insiders in administrative or other support positions in this sector included data entry clerks, office managers, customer service representatives, claims developer clerks, and general clerical and public assistance personnel. These are not positions generally thought of as "trusted" positions with access to classified information that may require extensive backgrounds to obtain. In this sector, however, insiders were mainly employed in these types of positions, at all levels of government, and used their access to personal data such as social security numbers and dates of birth to their benefit. Insiders reduced fines and cleared negative personal information for payment. Insiders also accessed and altered personal data that allowed for the generation of false documents to include drivers' licenses, social security number-related documents, and other identity documents.

At the time of their actions, some insiders were experiencing at least some level of financial difficulty. For some, adverse changes in their respective financial situations and/or status were compelling enough by ITS definitions to be considered triggering events for their damaging actions. Other insiders claimed their actions were altruistic in nature, yet nevertheless charged a fee in exchange for altering data to benefit other individuals.

Collectively, these findings suggest that access to this type of information may increase the chance of an insider incident. Personal information to include an individual's social security number, full name, date of birth, and address(es) is highly marketable. Organizations should recognize that employees who have access to personal data are in a position to sell this access. Ethics training and employee contracts can reinforce the sensitivity of this information and the responsibility entrusted to individuals who hold these positions.

The Incidents

Pre-Incident Planning

Key Findings
- The majority of insiders planned their actions.
- Others were aware of, involved in, or benefited from the insiders' illicit activities.

Implications
- Opportunities exist for earlier detection of illicit insider activities.
- Establishing a formal process for reporting and sharing information may encourage employees to alert employers of potential insider activity.

Opportunities exist for earlier detection of illicit insider activities. In the majority of these cases, others had knowledge of the insider's plans or colluded with the insider to perpetrate the incident. Insiders also had communications with others that may have assisted in furthering the incidents. In a number of cases, co-workers had knowledge of the insiders' activities through rumor or observation of questionable behaviors. In one case, a clerk was observed utilizing the computers at work to gain access to a specific individual's records for personal use. As part of her normal duties, the employee had authorized access to individuals' private addresses and contact information. However, the clerk was observed by co-workers accessing the marriage license, driver's license and other official records of an individual then was overheard passing this personal information to others. The clerk's activities were not reported until an investigation was initiated.

Government sector insiders conspired with others to carry out their illicit activities in just over a third of the cases examined, and most of this activity was initiated prior to the incident. In these cases, the insiders were not the only beneficiaries of the incidents. Co-workers, friends, family members, and other individuals paid the insiders to gain information or to have information altered in their files. For example, a husband and wife who were co-workers in a motor vehicle department conspired to collect payment from individuals with suspended licenses to re-issue the licenses and clear the records.

These findings suggest that opportunities exist for detecting insider incidents within this sector before damage to the organization occurs or for intervening in an incident to reduce the extent and duration of the damage.

Establishing a formal process for reporting and sharing information may encourage employees to alert employers of potential insider activity. Encouraging employees to express concerns about or knowledge of abnormal or illicit behavior and activities may help to provide information or clues regarding another employee's intent to harm. In addition, establishing processes and procedures to respond to employees' concerns also may help to identify individuals' activities within an organization prior to an actual incident. Developing a formal process for reporting and sharing information in the workplace is important whether the information provided is to be attributed to its source or reported anonymously. Employees should be informed of the process and encouraged to report suspicious or inappropriate behavior.

Procedures should also be developed for allowing various departments within the organization to share information regarding problematic or unusual employee behavior. Representatives from management, security, human resources, information technology, and legal counsel could benefit from sharing information they have learned regarding particular behavior of concern.

Technical Details of the Incidents

Key Findings
- Most of the insiders had authorized access at the time of their malicious activities.
- Access control gaps facilitated most of the insider incidents.
- Most insiders modified or deleted information using only user commands.
- Some insiders used technical means for compromising accounts or carrying out their malicious activities.

Implications
- Access control should be designed, implemented, and enforced at the enterprise level for all business practices. This includes not only technical controls for the network, systems, applications, and data/files, but also encompassing policies, procedures, and employee security awareness training.
  - Password and account management policies could close some access control gaps.
  - Access control should be carefully designed and implemented using the principle of <u>least privilege</u>.
  - Configuration management and <u>characterization procedures</u> could detect download, installation, or release of malicious code.
  - System logs should be directed to a secure location and backed up to ensure that all actions can be traced back to an individual user.
  - System vulnerabilities can facilitate malicious activity.
  - Periodic security awareness training could eliminate some compromises.

Access control should be designed, implemented, and enforced at the enterprise level for all business practices. Access control is often thought of as a technical function performed by an organization's IT group. However, insiders in this report exploited a wide variety of vulnerabilities and weaknesses in access controls to carry out their malicious activities.

These access control gaps included
- policy or procedural oversights or violations such as sharing passwords, leaving a computer logged in without a screen lock, or keeping an employer's laptop following termination
- social engineering resulting in password sharing
- poor implementation of access controls providing employees with excessive capabilities not needed to do their jobs
- insufficient technical controls enabled insiders to violate separation of duties and business policies (See Separation of Duties implication discussion below)
- system configuration that did not provide the ability to associate all actions with an individual user

- deficient account management practices that enabled the insider to utilize another account for his actions or create a backdoor account for later use
- ability of a technical insider to use technical methods to override access controls without detection
- system vulnerabilities that allowed technical insiders to use their specialized skills to override access controls without detection

Organizations should carefully design access control measures with an enterprise approach to information security. Access control includes not only technical controls at the network, system, application, and file/data level, but also requires policies, procedures, and employee security awareness training. In addition, access control should be an integral part in designing the organization's business policies.

Password and account management policies and procedures could close some access control gaps. In some incidents, insiders were able to carry out their malicious activities due to poor password and account management policies, procedures, and technology.[48] Some incidents were facilitated by passwords being routinely shared among employees to enhance productivity by overcoming the obstacles posed by role-based access control. In other incidents, the insiders deliberately set out to obtain other employees' passwords to carry out their illicit acts. Insiders also used shared accounts in some incidents for which multiple employees legitimately knew the passwords.

Policies should be instituted prohibiting sharing of passwords among employees. In addition, policies and technology should be used to require employees to choose strong passwords.[49] In at least one case the insider used a password cracker downloaded from the Internet to obtain passwords from other employees.

Account management should be implemented to formally track all accounts. Additionally, all employees who have passwords to access shared accounts should be tracked. Termination and transfer processes then can disable access to all accounts effectively based upon this information.

Access control should be carefully designed and implemented using the principle of least privilege. The principle of least privilege means that each employee should have only the access needed to perform his or her job functions. Some of the government sector insider incidents were carried out by insiders who exploited the limits of authorized access that their employers were unaware these insiders possessed. In other incidents, organizations permitted employees to retain access either following transfers within the organization or after termination of their employment. Procedures

---

[48] The second paper in the Insider Threat Study series expounded on the importance of these issues in preventing insider threats. Available on-line at http://www.cert.org/archive/pdf/insidercross051105.pdf and http://www.secretservice.gov/ntac/its_report_050516.pdf

[49] A strong password is one that is difficult for humans and computer programs to guess. For example, longer passwords are stronger than shorter ones. In addition, passwords should contain a combination of letters, numbers and symbols, and contain both uppercase and lowercase letters. Strong passwords also do not contain words that can be found in a dictionary. See http://www.cert.org/homeusers/HomeComputerSecurity/#6 for a discussion regarding strong passwords.

for transfers should be carefully designed to ensure that employees do not retain access to information or systems from their previous positions for which they no longer have a valid need. Termination procedures should be carefully designed. Findings in this report suggest that completely disabling access is warranted following an employee's termination. In one case, an insider was allowed to retain her employer's laptop following her termination. Although her electronic access had been disabled upon her termination, she was able to use the laptop to access the system and commit sabotage.

Organizations should take the time to design access control at the network, system, application, and data/file levels. Insiders have been shown to take advantage of vulnerabilities at many different levels. Access control should be implemented in multiple layers. Access to an application is one step in the access control process. Access to data within the application also must be carefully controlled, so that each user can only access the data for which he or she is responsible. Likewise, role-based access control can be used to control access to functions within an application, but access control at the data level should also be employed so that each user can still only access data within his or her area of responsibility. Finally, formal termination and transfer procedures should be implemented to ensure that access is modified or disabled appropriately.

Configuration management and characterization procedures[50] could detect download, installation, or release of malicious code. Malicious actions by some of the technical insiders in this report could have been prevented or detected earlier if the organizations had effectively implemented characterization procedures and configuration management. Characterization procedures are instituted specifically for detecting changes to the organization's software, hardware, and information assets. Configuration management systems are implemented to track and control changes to systems or applications. Used together, these practices could have led to early detection of several insider actions.

One insider modified the program used by employees for changing their passwords so that their new passwords were saved in a file unencrypted and accessible only to him. He also modified the source code for a critical function in a mission critical business application to turn off an automatic security notification that would have alerted them to his fraudulent activity. These modifications were not discovered until an external customer reported suspicion of criminal acts and an investigation was initiated. Interestingly, the organization in this case did use a configuration management system for tracking and controlling all program changes. After the insider's criminal acts were discovered, logs from that system were used to determine the changes the insider had

---

[50] Characterization procedures: A trusted baseline is established for each machine on the network, stored in a secure location, and periodically compared to the current "footprint" or configuration of each machine that implements that baseline. Unexpected files or changes to files revealed by this comparison can be analyzed to determine whether they are legitimate changes to the baseline or rather, malicious code. The release process for any new files must include an update to the trusted baseline. For a complete description of security improvement practices for characterizing software, hardware, and information assets see: http://www.cert.org/security-improvement/practices/p091.html

made to the programs. Had they used characterization practices they would have detected the changes much sooner. In addition, if they had routinely checked the configuration management system logs for all changes to critical programs and utilities they could have detected the changes much quicker.

As the above example illustrates, configuration and change management procedures and software do not provide a foolproof solution. They require strict monitoring, follow-through, and separation of duties. If these procedures are implemented effectively, however, they can detect otherwise obscure system changes or releases of new code. A comparison of system modifications to previous versions can highlight the insertion of malicious code. In addition, a configuration management system that enforces separation of duties, requiring separate authorization for release of changes to critical files, can prevent insiders from releasing malicious code in the first place.

Characterization procedures and configuration management are not only useful for detecting technical changes, but also for detecting simple changes to files that could be made by any insider. For example, a college intern played a practical joke on his coworkers by embedding libelous information in one of their web pages. The "joke" was not discovered until the intern returned to college at the end of the summer, when the agency was contacted by general counsel for the organization that was the subject of the libelous text. The modified text could have been detected and flagged in a timely manner by characterization procedures and the text recalled immediately.

System logs should be directed to a secure location and backed up to ensure that all actions can be traced back to an individual user. Some of the technical insiders in this report came very close to successfully carrying out their malicious activities without being identified and caught. When configuring their systems, organizations should consider the importance of the system logs when investigating any security incidents, as well as the threat posed to those logs by their technical users.

One insider was able to plant a logic bomb into a system utility, edit his supervisor's ".profile"[51] to frame him for the destruction, and edit system logs to delete all evidence of his actions. In an interview with this particular insider he stated that the organization used "wide open sudo,"[52] which enabled any user to perform any system administration functions. He also said that the system logging was configured so that he was able to edit all of the logfiles and delete all traces of his actions except those that he purposely modified to point to his supervisor. However, he forgot about a single system log, which took months for an external forensics expert to locate.

It is important that organizations realize that their system logs can provide valuable evidence in case of an insider incident and configure their systems accordingly. System logs should be directed to a secure location and backed up so that they are protected

---

[51] In UNIX, the .profile is a file in a user's home directory that contains commands that are executed when that user logs into the computer.
[52] *sudo* is a UNIX command that allows users to run programs with the security privileges of another user (normally the system's superuser). See http://en.wikipedia.org/wiki/Sudo for more information.

from manipulation, and can be restored in case of system failure to trace all activities to their sources.

Technical vulnerabilities can facilitate illicit activity. Some of the technical insiders in this report took advantage of technical system vulnerabilities to commit their illicit acts. It is important that organizations realize that

- system vulnerabilities provide a tactical opportunity for both external attackers and insiders to carry out illicit activity
- the organization's network and system architecture and configuration decisions can create new vulnerabilities

In one case, the insider took advantage of an unpatched system vulnerability to commit his activity.[53] Although this technique was only used in a single case, it bears mention because patching system vulnerabilities is a crucial aspect of any organization's information security strategy. System vulnerabilities provide an avenue for unauthorized access to an organization's system. External attackers must first locate the system with the vulnerabilities, but system administrators inside an organization know which of their organization's systems are vulnerable. Therefore, should they decide to attack their own organization, system administrators in an organization have an easy mechanism for gaining anonymous and unauthorized entry to the organization's systems at any time, from inside or outside.

Organizations routinely assess the risk of an *external* attacker exploiting a system vulnerability to obtain unauthorized access to their networks. However, it is important that organizations realize that their own system administrators are aware of their patching policies and practices, and therefore are aware of which of those many vulnerabilities are exploitable from outside the organizations' networks. This "insider knowledge" can give them the ability to use an external account to gain access to the system, making identification of the perpetrators much more difficult.

In addition to vulnerability patching, other network and system architecture and configuration decisions made by an organization can increase risk of insider threats. For example, the organization mentioned above that implemented "wide open sudo" provided an easy avenue for their insiders to commit illicit activities. These types of technical decisions should be considered carefully and should be reviewed by technical staff with sufficient expertise to adequately assess the potential consequences.

Periodic security awareness training could eliminate some compromises. Some of the incidents in this report were facilitated by individuals who were not aware of the potential implications of their actions. Periodic security awareness training for all employees would ensure that employees not only understand the security policies and

---

[53] The CERT website contains information on vulnerabilities and current activity: http://www.cert.org/stats/cert_stats.html The number of vulnerabilities reported to the CERT Coordination Center® in the first three quarters of 2006 reached 5340, compared to 5990 for the entire year of 2005 and 3780 in 2004.

procedures of their organization, but also the reasoning behind them, and the potential repercussions to the organization and employees if they are violated.

Findings from the ITS have shown that employees should be trained on fundamental issues such as not sharing passwords and not leaving their computers logged-in while unattended. They need to understand that system security is based upon each employee having an account that cannot be used by anyone else. System, application, data, and role-based access controls are all built upon this premise. In addition, if an employee's account is used for malicious activity, then all of the evidence will point to that employee as the perpetrator, not the person with whom the employee shared his or her password.

Employees should also be trained in the concept of social engineering. Although social engineering occurred in only two cases in the government sector, it bears mention because it is a tactic that can be utilized to manipulate employees by persons both internal and external to the organization. No matter how tight the technical security controls implemented by an organization, if employees are unaware of the dangers and tactics involved in social engineering, they may unwittingly provide access, assist in concealing malicious activity, throw suspicion on themselves, or destroy evidence. For example, in one of the two social engineering cases, the insider convinced a coworker to erase all but a handful of backup tapes that documented the insider's illicit activity. The insider was able to elicit the coworker's cooperation on the ruse that the organization was installing a new backup system and the tapes were no longer needed. The coworker was unaware of the insider's efforts to destroy evidence of his actions. Organizations can consider developing procedures for employees to report suspected attempts at social engineering, including intimidation into revealing passwords and excuses by other employees for using an employee's computer.

In addition, in this sector the actions of insiders were often detected by co-workers, supervisors, outsiders, and victims, some of whom directly informed internal investigators and law enforcement of their concerns. A strong security awareness program can inform employees about the behaviors and actions they should consider suspect by fellow co-workers.

Business Process Issues Related to the Incidents

Key Finding
- Some insiders exploited weaknesses in established business processes or controls such as inadequate or poorly enforced policies and procedures for separation of duties.

Implications
- Business practices and oversight controls should provide for and enforce separation of duties' policies and procedures as checks and balances against insider threats.

- Formal procedures for validating the integrity of information from its original data source could detect collusion among multiple insiders.
- Technical controls like role-based access control should be implemented to enforce separation of duties.
- A combination of manual and automated processes should be implemented to detect business process violations by technical staff.

Business practices and oversight controls should enforce separation of duties as checks and balances against insider threats. Half of the ITS government sector insiders exploited a deficiency or weakness in a business process to commit their activities. Ineffective implementation of separation of duties provided the opportunity exploited by some insiders. When separation of duties is not built into the business process, is flawed, or inadequately enforced, an easy mechanism exists for insiders to commit illicit activities.

One insider, responsible for entering and maintaining vendor information in a city's inventory and procurement system, entering purchase requisitions, and maintaining inventory data, exploited the lack of separation of duties to defraud the city of $264,000. In carrying out his activity, this insider entered a fabricated vendor, created purchase requisitions for that vendor, and manipulated the inventory data to conceal the fact that no goods were ever actually received.

Other insiders took advantage of subtle flaws in their organizations' business processes. In one case, supervisors were delegated the approval role in the system, but also had the ability to manipulate the original data that they were approving. While there may have been good reasons for providing the supervisor the ability to perform both functions, the possible repercussions were not carefully considered. The privileges of multiple roles gave the supervisor a path to circumvent separation of duties using his authorized access.

Strong business processes usually include a combination of manual procedures and automated technical processes and controls. Manual procedures alone can often be manipulated for illicit intent by insiders, as mentioned previously in this report. Likewise, technical controls alone are not sufficient for ensuring integrity in a business process. For example, in the case of the college intern mentioned previously, the process used to make changes to a state's website was carefully designed, with technical controls implemented so that only a small group of privileged users could actually publish files to the website. However, the process did not include a formal review of the pages before they were published, which enabled the intern to embed the libelous information in one of their web pages, undiscovered until the intern returned to college at the end of the summer.

Finally, in the two social engineering cases in this sector, both insiders manipulated other employees to assist in circumventing separation of duties. For example, one insider told a coworker that his computer froze so he needed to use the coworker's computer. In the other case, a supervisor intimidated a subordinate into revealing his

password. In both cases, the insiders were able to circumvent separation of duties by using another employee's account to perform functions not authorized for their own accounts. This again illustrates the value of security awareness training to educate employees on the importance of separation of duties, how it is implemented, and how separation of duties can be circumvented.

Formal procedures for validating the integrity of information from its original data source could detect collusion among multiple insiders.[54]
A few of the insiders in this report were able to defeat the intended benefits of separation of duties, whether it was enforced loosely via policy or through strict technical controls, by colluding with other insiders. Prevention and detection of these incidents were difficult, as multiple insiders used their legitimate system access to perform the tasks they performed everyday to carry out their illicit acts.

Effective separation of duties requires validation of the integrity of data as it flows into, through, and out of a system. In many systems data is manually entered into a database by an employee. That data is then examined, acted on, and/or approved online by someone with a different role. When the second employee indicates that the data is ready to move to the next stage of the business process, the status of the data in the database is changed accordingly. The data flow might also move out of the system to an external source. The final step in the process could be generation of a check, an online transfer of money from one system to another, or printing of an official identity document.

Business processes frequently are designed with the assumption that all steps in the process will be performed correctly and legitimately. When final approval for a process or transaction is entered, the user might assume that each employee who preceded him in the process did their job correctly, entering data correctly and checking it for accuracy. A possible solution is to have the business process designed to require that the final approver trace the data all the way back through the system to the original source. This duplication of effort obviously comes with a cost, and should be weighed carefully against the criticality of the data and the potential impacts of either accidental oversights or intentional malicious activity by multiple insiders.

Technical controls like role-based access control should be implemented to enforce separation of duties. Some of the organizations in this report appeared to include separation of duties in the design of their business processes, but enforced it via formal or informal policy rather than technology. Separation of duties increases the difficulty in carrying out insider incidents. Enforcement via technical controls, such as role-based access control, adds yet another degree of difficulty that must be overcome by insiders in carrying out their malicious activities. Implementing technical controls adds one more layer of protection against insiders.

---

[54] These procedures would also be effective in detecting malicious activity by insiders working alone. However, the intent of this commentary is to discuss how collusion among multiple people could be detected.

For example, while investigating a nonexistent child care provider accidentally discovered in the database, agency personnel found that two different insiders had been defrauding the agency. This was accomplished by entering a relative as a child care provider, entering false claims, and then splitting the checks that were sent to the relative. Although the insiders were carrying out their acts during the same time period at the same agency, they insisted that they were not aware of the other's actions. Coincidentally, they had both taken advantage of the fact that while only the supervisor was authorized to enter new child care providers following successful background checks, there were no technical controls to prevent any user from entering them into the system. If the function for entering new providers had been technically restricted to only users with a supervisory role it would have been much more difficult for the insiders to carry out their fraud.

A combination of manual and automated processes can help to detect business process vulnerabilities exploited by technical staff. While role-based access control is an effective mechanism for protection against insider threats, system administrators and other privileged users typically sit atop the power structure of role-based access control, granting and restricting access for all other personnel. In addition, role-based access control is often implemented in source code and/or application databases; technical staff often has the ability to modify source code, databases, and the system-level data upon which the role-based access control relies.

Safeguards should be instituted to protect the organization from a technical insider who might modify source code or user roles in a database to circumvent the role-based access control. While these specific types of exploits were only found in a few cases in this study, the ease by which they were committed and concealed is reason for concern. It is much more difficult to detect these types of violations by technical staff, because they are not only aware of the security mechanisms in place to detect violations, but they themselves are often responsible for designing, implementing, and enforcing them. Often, a combination of manual and automated detection mechanisms is necessary for detecting malicious activity by technical staff. For example, a configuration management system will log all changes to a system but cannot determine whether changes are legitimate; that analysis requires a manual process.

Detecting the Incidents

Key Finding
- Insiders were detected and identified by a combination of people, processes, and technologies.

Implications
- Agencies should have procedures for collecting and handling all information that indicates possible insider threats, whether the information originates from people, processes, or technology.
- Recognizing potential insider incidents requires a strong internal system of controls.

- Physical security, personnel security, and cyber security information should be shared with affected groups within the organization to detect and identify insider threats.

Agencies should have procedures for collecting and handling all information that indicates possible insider threats. Insider threat and vulnerability information can come from sources both internal and external to an organization, and from people, processes, and/or technology. In some incidents reviewed, multiple sources alerted officials to an insider threat. These sources included
- audit findings
- business and financial record errors and deletions
- public reports and complaints
- public informants
- law enforcement investigations
- direct observation by employees

Any information that indicates that an employee or contractor is planning to carry out malicious activity against the organization, and insight into how the insider plans to carry out the incident should be investigated by the organization. Vulnerabilities in business processes, key technologies, policies, or operational procedures should be considered seriously as such vulnerabilities could be exploited by an insider as was the case in many of the successful insider incidents studied for this report.

These findings suggest that government agencies should be prepared to collect, take action on, and maintain data on tips, reports, and other threat information received from any source. Agencies should prepare for and develop procedures to handle information reported both formally and anonymously; they should anticipate and prepare to handle information received via multiple communication channels, such as email from, or reports by auditors; phone calls from overseas law enforcement agencies; visits or phone calls from an internal agency accountability official; communications from a general counsel for a victims services organization; and so on. Procedures should be in place so that employees who discover this information are aware of how to route the information to the appropriate department, security office, or supervisor.

Recognizing potential insider incidents requires a strong internal system of controls. Technical insiders described in this report used their skills to circumvent the legitimate business process and exploit deficiencies in security mechanisms and controls. Findings suggest that agencies should develop ways to recognize potential insider threats based on the results of auditing, monitoring, and tracking.

In some incidents, agency's regular internal systems of controls and security safeguards, such as periodic audits, reviews of database records, or paper files, detected inconsistencies in recordkeeping. Subsequent examination of information security logs led organizations to uncover direct evidence of the specific manner in which the malicious activity was conducted. In most incidents multiple system logs identified a specific insider as the perpetrator of the crime. Collectively, these findings

demonstrate the usefulness of regularly reviewing application, system, and network logs for events that are outside of the norm and argue strongly for routinely tracking the "online" behaviors and computer use of employees.

Physical security, personnel security, and cyber security information should be shared with affected groups within the organization to detect and identify insider threats. Successful investigation of illicit insider events requires the collection and analysis of all available information to determine the specific actions and actors involved in the incident. This information should include any records that the target organization may have for employees whose actions or behavior raised suspicions or concerns, or required formal or informal intervention. The ITS found that in some insider incidents examined, target organizations' officials did not share information concerning employees with prior arrests or records of performance- or behavior-related problems with internal or external investigators.

The evidence collected during an internal response to an incident must be protected and preserved according to law enforcement procedures or the evidence will not be admissible in court. Since evidence is sometimes collected from different departments in an agency, procedures must be in place to standardize and facilitate collection, storage, and reporting. Contacting law enforcement at the initial stages of the investigation is suggested unless well trained and experienced forensics experts are available internally.

In some incidents, physical security records, computer system information such as logs, and personal observations were instrumental in identifying the insider. In one case an employee observed the insider in a computer room on the day that database records were deleted. Although the employee did not witness the insider committing the crime, the sighting in the computer room, combined with the fact that only the insider and his supervisor had knowledge of the password necessary to damage the records, provided the evidence needed for a conviction.

Consequences of the Incidents

For Insiders

Key Findings
- Insiders faced criminal charges in most cases.
- Insiders did not anticipate the severity of the consequences for their illicit activities.

Implication
- Employee security awareness programs that address organizational response to policy violations may be beneficial.

Employee security awareness programs that address organizational response to policy violations may be beneficial. The majority of insiders reported that they did

not consider possible negative consequences they may face as a result of their activities. In most of the cases in this sector, organizations took some type of punitive action either internally or externally against the insider for his or her illicit activities. In many of these incidents, criminal charges were filed against insiders at both the state and federal levels; however, insiders faced state charges slightly more frequently.

In addition to legal and official consequences, these insiders often faced personal repercussions such as difficulty obtaining future employment and financial struggles. One insider interviewed discussed his regrets and the serious consequences of his actions. He explained that his negative actions, which took five minutes to carry out, set him back five years and dramatically impacted his life. Due to a felony conviction for his actions, he continues to have trouble obtaining long-term employment. The insider advises that his actions, "ruined his shot at life," and were not worth committing.

These findings suggest that organizations could benefit from developing employee security awareness programs that effectively communicate an organization's acceptable use policies and the intent to pursue and prosecute crimes against employees who violate these policies. Employees may be discouraged from committing illicit acts if they are made aware of the potential legal, professional, and personal consequences they may face.

For Target Organizations

Key Finding
- Insider actions affected federal, state, and local government agencies with the major impact to organizations being financial loss resulting from damage to information or data.

Implication
- Enhancing the quality of information security policies, practices, and technologies is important.

Enhancing the quality of information security policies, practices, and technologies is important. Agencies in this sector appear to have strived to adhere to government requirements for information security policies, practices, and technology. Most of the victim agencies in this report had acceptable use policies, communicated the policy via security awareness programs, conducted audits to detect illicit activity, and responded to abuses with sanctions. While agencies conformed to requirements, the mere existence of these practices and programs may not be sufficient.

Employees in this sector were able to commit fraud, theft of confidential and proprietary information, and identity theft, by simply altering or viewing electronic information. In the government sector, where strict certification and accreditation (C&A) requirements exist, more important than being able to check off the requirements on the C&A checklists is attention to their comprehensive and thorough implementation. Agencies can benefit from considering the adequacy of their implementation of these policies,

practices, and technologies. Furthermore, security and risk assessment programs should put at least as much emphasis on threats from inside as from outside.

Other Consequences

Key Finding
- A minority of cases had a noticeable impact on the general public and demonstrated the potential for risks to homeland security.

Implication
- Government employees have the ability and opportunity to commit offenses that can result in serious consequences to an agency, the general public, or homeland security.

Government employees have the ability and opportunity to commit offenses that can result in serious consequences to an agency, the general public, or homeland security. Insiders at all levels of government with access to sensitive and confidential information can pose a vulnerability. For instance, the document fraud cases in this sector required only minimal technical skill and were executed by employees occupying various positions ranging from entry-level clerks to supervisors. This activity involved only a minority of the cases in this sector, but the resulting consequences are worth noting. The consequences from these cases included the following:
- Over 200 illegitimate federal identity documents were issued to illegal aliens, permitting them to work and live in the U.S; some were granted asylum when they had been marked for deportation.
- Over 1300 fraudulent state driver's licenses were issued. A majority of these were issued to illegal aliens. Some of the licenses displayed the social security numbers of other, legitimate license holders.
- Nearly $300,000 in credit card fraud affecting innocent persons was committed as a result of these falsely issued federal and state identity documents. In addition, 2500 queries of personal and confidential information run by one insider were eventually tied to an unknown amount of credit card fraud.

The insiders' goals in these incidents were mainly financial, but the resulting consequences were sometimes broad as noted above. The insiders did not necessarily consider the far-reaching repercussions of their actions. Although insiders colluded with foreign nationals in only 13% of cases, these co-conspirators usually benefited financially and gained improved citizenship status. Employees who have access to confidential or sensitive information may be susceptible to influence from persons external to the organization whose intentions are malicious.

ITS researchers have exercised caution in reporting on, and drawing conclusions from, the findings of the relatively small number of cases that could be identified and analyzed for this sector, especially the incidents involving document fraud and the release of personal information. Rather than draw conclusions from these incidents, they serve as

a reminder that organizations in the government sector, whether they operate at the local, state, or federal level, protect and manage sensitive information that if abused or stolen can cause damage well beyond the scope of the original incident.

SECTION 4: CONCLUSION: REFLECTIONS ON THE FINDINGS OF THE ITS GOVERNMENT SECTOR REPORT

With the completion of this report, ITS researchers have examined illicit insider cyber activity in the banking and finance, information technology and telecommunications, and government sectors; and incidents of sabotage that occurred across critical infrastructure sectors. The findings from each report in the study have contributed to information on the insider threat issue and offered unique insight particular to the relative sector or activity examined.

The findings and implications provided in this report offer insight into employees who commit illicit cyber acts within the government sector. While the relatively small number of insider cases necessitates caution in acting on and drawing conclusions from the study, it doesn't diminish the value of the information. For instance, researchers found that in many cases insiders used authorized access to alter or obtain an individual's personal data in some manner. This finding helps us better understand how access to identity-related data might contribute to insider activity in this sector. Another finding, many insiders exploited weaknesses in business processes to carry out their activities, helps us better understand how these incidents were perpetrated. Two other activities identified in this sector, identity document fraud and collusion, necessitate comment since they can potentially have consequences for the general public and homeland security. This section highlights the major findings and implications from the analyses, and offers additional considerations for the prevention of insider activity.

Key findings and implications for this sector

Employees primarily held administrative and support positions, and tended to use their access for financial benefit. They did not share common demographic descriptors; however, nearly half of employees did exhibit some odd or concerning behavior in the workplace. Some employees also planned their activities in collusion with others.

Agencies at all levels of government were targets of insider threat. Federal, state, and local government experienced incidents of fraud, sabotage, and theft of confidential information that occurred because of similar vulnerabilities in business practices and access controls. In addition, the primary harm to agencies occurred in the form of damage to or loss of data.

Considerations for the government's ability to secure information

Many agencies in the government sector, whether they operate at the federal, state or local level, manage sensitive information. For example, submission of personal and confidential information is mandated on income tax filings and applications for unemployment, social security, and subsidized or affordable housing assistance benefits. This information is also used to facilitate the delivery of optional services to citizens and businesses in areas such as health care, grants and loans, social programs, education, and disability benefits.

By virtue of their positions, many employees of government agencies have access to electronic systems containing private information on other public agencies, U.S. businesses, and U.S. citizens. In over half of the cases detailed in this report, insiders were involved in schemes to use or sell identity-related data. In some of the fraudulent federal identity document cases, recipients received benefits from the U.S. with all the rights afforded to individuals who are legally entitled. Also, some victims of credit card fraud had their social security numbers compromised leaving them vulnerable to identity theft. When employees reveal confidential and proprietary information entrusted to their respective agencies, their actions can potentially result in serious unintended consequences to the affected agencies, the general public, or homeland security.

Electronic storage of citizens' confidential information necessitates accurate, reliable, and confidential record keeping within government databases and computer systems. Policies and technical controls are implemented to provide a safety net for critical data; when insiders violate these tenets they jeopardize the relationship between the agency and the customer, sometimes impacting confidence and trust beyond the victim. Government agencies at all levels need to remain vigilant against the potential impacts of insider incidents on public trust and the citizens' confidence in government services. It is important that government organizations have measures in place to safeguard data from theft and abuse.

Considerations for risk assessment
Government agencies are responsible for the confidentiality, integrity, and availability of the information for their customers, partners, and employees. The findings in this sector suggest that government agencies should have proactive strategies to protect information entrusted to them to include continuous and standardized risk management processes. In addition, the risk from insiders should be included as an essential data element in assessments.

Federal agencies are required to comply with Title III of the E-Government Act of 2002 known as the Federal Information Security Management Act (FISMA). FISMA outlines requirements for security management using an agency-wide, risk-based security program. FISMA calls for "periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency."[55] Periodic risk assessments are required, but risks from insider attack are not given specific consideration in addition to other threat sources.

Similarly, some states have enacted laws and standards requiring risk assessment and other diagnostic techniques to determine the security of systems and information for their government agencies. The National Infrastructure Protection Plan (NIPP) also provides a coordinated risk management approach for federal, state, and local agencies. However, insider threat is missing as an essential data element in many of

---

[55] Federal Information Security Management Act of 2002, H.R. 2458-48, § 3544.(b)(1).

these approaches and the risk assessment process is not standardized across all states.

In the end, insiders jeopardize 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.

Considerations for additional research
The nature of the insider threat across all sectors since 2002 may have changed due to critical issues that were not previously prevalent. Future research on insider threat issues that might be helpful to consider are trends in outsourcing, identity theft, and terrorism. Other research areas include technological advances and the new vulnerabilities they present that can be exploited by insiders. Of note, there are likely technological advances that may have already corrected some of the vulnerabilities observed in the ITS reports.

Finally, the cases included in this study were either investigated by the Secret Service or were identified through the media making it impossible to assess how widespread these experiences and consequences are in the broader government sector. Future research is possible only if organizations share information on insider incidents, and on policies, practices, and technologies successful in detecting or preventing incidents. This information can be useful in developing broader strategies for mitigating insider threat risk, as well as defining requirements for tools, training, and other products for the prevention or early detection of insider threats.

APPENDIX A: Tables

TABLES 1 – 3: INSIDER RELATED TABLES

Table # 1 Insider Demographics

Demographics	N=38	100%*
Gender		
Male	19	50%
Female	19	50%
Marital Status (n=31)		
Married	15	48%
Single	9	32%
Separated	3	10%
Divorced	3	10%

* +/-1% due to rounding.

Table # 2 Insider Age Range

Is information available on insider age?	N=38	100%
No	5	13%
Yes	**33**	**87%**
Age	**N=33**	**100%**
25 & Under	3	9%
26 - 35	13	39%
36 - 45	13	39%
46 - 55	4	12%

Table # 3 Insiders Facing Federal or State Criminal Charges

Insider Charged Criminally?	N=38	100%*
No	4	11%
Yes	**34**	**90%**
Charges Filed	**N=34**	**100%**
State	18	53%
Federal	16	47%

+/- 1% due to rounding.

TABLES 4 – 9: ORGANIZATION AND INCIDENT RELATED TABLES

Table # 4 Type of Government Agency: Incident by Agency Type

Type of Government Agency	N=36	100%*
Local	14	39%
Federal	11	31%
State	11	31%

* +/-1% due to rounding.

Table # 5 Size of Affected Organization by Number of Employees[56]

Number of Employees	N=28	100%
1-100	5	18%
101-500	5	18%
501-3,000	4	14%
3001-10,000	4	14%
10,001-50,000	5	18%
Over 50,000	5	18%

---

[56] Information available on only 28 of 36 organizations.

Table # 6 Incidents by State

State	N=36	100%
Florida	4	11.1%
Texas	4	11.1%
California	3	8.3%
Pennsylvania	3	8.3%
Kentucky	2	5.6%
Louisiana	2	5.6%
Maryland	2	5.6%
New York	2	5.6%
Rhode Island	2	5.6%
Virginia	2	5.6%
Colorado	1	2.8%
District of Columbia	1	2.8%
Georgia	1	2.8%
Illinois	1	2.8%
Indiana	1	2.8%
Kansas	1	2.8%
North Carolina	1	2.8%
Nebraska	1	2.8%
Ohio	1	2.8%
West Virginia	1	2.8%

Table # 7 Incidents by Year of Initial Damage

Year of Incident	N=36	100%*
1996	6	17%
1997	7	19%
1998	6	17%
1999	5	14%
2000	6	17%
2001	4	11%
2002	2	6%

* +/- 1% due to rounding.

Table # 8 Financial Damage: Dollar Loss to Agencies[57]

Did agency experience financial damage?	N=36	100%
No	9	25%
Yes	**25**	**69%**
Don't Know	2	6%
Financial damage where known	**N=24**	**100%***
$1-$20,000	9	38%
$20,001-$50,000	5	21%
$50,001-$100,000	4	17%
$100,001-$200,000	1	4%
$200,001-$300,000	3	13%
$300,001-$400,000	0	0%
$400,001-$500,000	0	0%
$500,001-$1,000,000	1	4%
$1,000,001-$5,000,000	1	4%

* +/-1% due to rounding.

Table # 9 Law Enforcement Notification[58]

LE NOTIFIED	N=36	100%
No	3	8
Yes	**33**	**92%**
LE Agencies Notified	**N=30**	**100%***
Federal	10	30%
Local	9	27%
State	6	18%
Multiple Agencies	5	15%

* +/-1% due to rounding.

---

[57] Information available for only 24 of 25 organizations suffering financial damage.
[58] Information available for only 30 of 33 organizations that notified law enforcement.

APPENDIX B: Additional Case Examples

Exploitation of Weaknesses in Business or Operational Practices

Lack of Separation of Duties
A traffic court clerk was able to modify the court's database to remove fines for individuals, replacing them instead with a code indicating that there had been an error. She also was able to modify money orders or checks to be payable to herself. There was no separation of duties built into the business practice to require a supervisor's approval for correcting a stated fine or to ensure integrity in the financial process. The insider, who netted $1,800 for her illicit acts, was indicted for 15 counts of forgery, counterfeiting, embezzlement, wrongful conversion, and accessing a computer for fraud. She pled *nolo contendere*, was convicted, and received a five-year suspended sentence and five years probation.

Danger of an Operational Process That Relies on a Single Individual
The financial division manager for a parking authority was responsible for handling disputes regarding parking tickets. With no business controls over this process, it was very easy for him to mark tickets as voided in the system while pocketing the money that he actually collected in fines, or collecting the full amount of the fine, reducing the amount collected in the system, and keeping the difference.

Exploitation of Obscure Operational Process Flaw
Two insiders at a state agency that distributed food stamps were able to exploit an obscure weakness in the system to make over $70,000 in food stamp kickbacks. They issued food stamps to people who were not entitled to them or increased allocations in return for a certain number of food stamps, which they kept. They were able to execute this scheme because of a single weakness in the system they used: if a case was entered as "expedited" then the case could be executed without a supervisor's approval, and it did not require complete information, such as social security numbers. In addition, the insiders were able to modify these cases (53 cases in all) at will; after the food stamps were distributed they would mark the cases as "denied" so that they never showed up on any of the supervisor's caseload reports.

Use of Social Engineering to Circumvent IT Operational Practices
A manager in the IT department of a state agency, suspected that management had become aware of his ongoing fraud scheme. He instructed one of his staff to initialize the previous four weeks of backup tapes under the ruse that the agency was converting to a new system and that the old tapes therefore no longer would be useable. The initialization process wiped all data from the tapes so that it could not be recovered. By the time management became aware of what the insider was doing, all but a handful of tapes had been erased, making proof of his fraud much more difficult than it would have been otherwise.

Use of Collusion to Override Separation of Duties Controls
A state department of motor vehicles licensing agency used separation of duties to protect itself against insider fraud, requiring that all modifications to driver's license information be entered by a clerk and verified by a manager before it became effective. Two insiders colluded to

overcome those controls, modifying legitimate drivers licenses by replacing licensees' pictures with photographs of themselves and fake addresses. They then used those licenses to obtain credit cards in their victims' names with which they bought cars and other merchandise totaling $255,000 in value.

Use of Access Control Gap to Override Separation of Duties

A water meter reader for a state water department designed a scheme to lower or eliminate water bills for customers in exchange for a fee. He used his supervisor's computer when she was in the restroom to lower bills, a function authorized only for supervisors' accounts. Over 18 months he reduced bills by over $325,000 for 17 customers.

Exploitation of Weakness in the Software Development Process

The lead for a software development project refused to adhere to the organization's procedures for documentation and backups during software development. Management was aware of the insider's negligence, repeatedly requesting that he rectify the situation, but he ignored them with no consequences. At the end of the project, he wiped all files from his laptop – the only copy of the files that existed. Fortunately, law enforcement discovered an encrypted disk at his home containing the source code, but for several months he refused to decrypt the files and the organization was only able to run the executable version of the software. In the meantime, without access to the source code, the organization had no ability to make modifications or enhancements to the running version of the mission critical system.

Use of Access Control Gaps

Change in File Permissions to Facilitate Malicious Activity

An insider possessed privileged access to his organization's system. Although he should not have had access to certain system files, he used his privileged access to change the access rights on those files so that they were accessible to him. He then used that access to commit fraud against his organization for a total of nearly $63,000 over an 18-month period.

Danger of Allowing Access Following Friendly Termination

A project leader took a new position in a different department within the same organization. Because the termination was mutually agreeable, he convinced supervisors in his former department to permit him to retain an account on their system, although with lower access rights than before. That access combined with his knowledge of additional access methods on the network enabled him to repeatedly increase the access rights on his account, even as the increased access was discovered and corrected by the system administrator. Using the elevated access, he logged in after hours and accessed confidential personnel and payroll files.

Danger of Weak Passwords

A software developer worked for a subcontractor for the primary contractor on a large government project. This insider, who had become disgruntled because of increased security measures, downloaded a password cracking program from the Internet, copied the government agency's password file to his desktop, and executed the password cracker against it. He successfully broke 40 out of 160 passwords, including the system administrator password. Fortunately, he bragged about his knowledge of the system administrator password to the system

administrator, who immediately reported the security breach. An investigation ensued before the insider had a chance to use the passwords.

Creation of Backdoor Account Prior to Termination
After working as a contractor for a large government agency's subcontractor for about eight months, an insider received an offer for a permanent position with the subcontractor. A pre-employment drug test proved positive for cocaine, therefore the offer was rescinded. The insider, realizing that the drug test would be a problem, created a backdoor account. The account was used following his termination to delete printer drivers, change account passwords, and shut down the system for twelve hours.

Use of Long Dormant Account of Former Employee
The insider in this case worked as a subcontractor to a state government agency. The insider had system administrator access and physical access to the state agency's computer system. Over time, his employer lost the contract, and as a result his employment was terminated. Later, agency personnel noticed a series of intrusions into the agency's systems by an account that had belonged to a former employee and had been dormant for quite some time. Although it had been an unprivileged account, they noted that at the time of the intrusions it had full system administrator rights. During the intrusions, the insider changed user passwords and accessed email.

Use of Multiple Access Control Gaps Following Termination
A database administrator who left an agency under highly contentious circumstances attacked her former agency almost two months after her departure by exploiting a variety of access control gaps. First, she used an account and dial-in phone number that was only shared with certain trusted employees. Second, she used the username and password for another employee to log into the system; the organization's operating system provided easy access to all user passwords to users with system administrator access, which she had. Finally, she used a DBA account for which 15 employees knew the password to access the organization's database and delete a massive amount of critical data.

Detection and Identification of the Insider

Necessity of Both Manual and Automated Detection Mechanisms
To expound on the case summary from page 23, a manager in a state lottery's IT department was not permitted to access an application screen which allowed modification of lottery ticket data, but he did have access to the source code for the screen. He modified the source code, deleting the code that sent an automatic email to the security department anytime that screen was used to modify ticket information. He also changed his account privileges so he could access the screen, and then used the screen to change losing tickets he had purchased into winning tickets. Security email was not sent, enabling him to steal nearly $63,000 over a year and a half. Although the organization had automated logging in its configuration management system which logged the change to the source code, the organization had no formal auditing procedure for analyzing the logs. Therefore, the insider evaded detection for a long period of time.

Importance of Protecting Potential Evidence

A manager suspected of fraud was placed on administrative leave. Realizing that incriminating evidence was contained on his organization's backup tapes, he called one of his team members and told him that there was evidence on the backup tapes that would prove his innocence. The team member proceeded to obtain the tapes, took them home, and turned them over to the insider. The tapes were never recovered.

Importance of Protecting System Logs

A system administrator, who was reprimanded for frequent tardiness, absence, and unavailability at work, inserted a logic bomb onto his employer's production servers and set it to be executed in two different ways. In an effort to conceal his actions, the insider deleted all records of his actions from all system and network logs, removed history files, and constructed the logic bomb to overwrite itself after execution. Fortunately for the organization, the logic bomb was detected prior to detonation. However, the organization expended substantial resources to locate all instances of the logic bomb and conduct a complex forensics investigation.

APPENDIX C: Glossary of Technical Terms[59]

access controls: the rules and mechanisms that control access to information systems and physical access to premises.

authorized access: explicit permission to use.

backdoors: in computer and network systems, unauthorized means for gaining access to the system known only to the person who installed them.

characterization procedures: a trusted baseline is established for each machine on the network, stored in a secure location, and periodically compared to the current "footprint" or configuration of each machine that implements that baseline. Unexpected files or changes to files revealed by this comparison can be analyzed to determine whether they are legitimate changes to the baseline or rather, malicious code. The release process for any new files must include an update to the trusted baseline. For a complete description of security improvement practices for characterizing software, hardware, and information assets, see http://www.cert.org/security-improvement/practices/p091.html.

critical assets: an organizational entity essential to the organization's mission or efficient functioning.

configuration management: procedures or software for tracking releases and changes to software components so that previous versions can be recreated. It can also prevent unauthorized access to files or alert appropriate users when a file has been modified or released. Hardware configuration management can be facilitated through maintenance of a database containing information about the workstations, servers, bridges, routers, and other equipment on the network.

DNS (Domain Name System): translates domain names like www.cert.org into IP addresses.

FTP (File Transfer Protocol): a protocol and command used to transfer files from one computer to another.

IP address (Internet Protocol address): number used to uniquely identify computers on the Internet.

least privilege: each employee should have only the access needed to perform his or her job functions.

logic bomb: malicious code implanted on a target system and configured to execute after a designated period of time or on the occurrence of a specified system action.

---

[59] Many of these definitions are taken from the Information Security Glossary (http://www.yourwindow.to/information-security/).

password cracker: a tool used to recover passwords, usually by repeatedly guessing the password. Could be done to help a user recover a forgotten password, to gain unauthorized access to a system, or as a preventive measure to check for easily crackable passwords.

privileged users: users who have an elevated level of access to a network, computer system, or application. For example, system administrators, network administrators, and Database Administrators (DBAs) have the ability to create new user accounts and control the access rights of users within their domain.

production system: a system being used for business operations, as opposed to a system under development.

.profile: in the UNIX operating system, the .profile file contains commands that are executed when the user logs into the system.

remote access: the ability to access a computer or network from a distance without physical access to the facility in which the computer or network is located.

role-based access control: role-based access control restricts system functions to authorized roles, rather than individual users. Within a system, roles are created for various job functions. The permission to perform certain operations in the system is assigned to specific roles. Each system user is then assigned a particular role or roles, and through those role assignments acquire the permissions to perform particular system functions.

screen lock: security utility that lets users lock their computers so that the computers can only be unlocked with a password.

Script: scripts or programs can be written to execute a series of commands against the operating system, application, data, or network. A few examples of scripts or programs are UNIX shell scripts, Trojan horse programs, or password-cracking programs.

separation of duties: the process of disseminating the tasks and associated privileges for a specific business process among multiple users in order to prevent fraud and errors.

social engineering: gaining access through manipulation of a person or persons who can permit or facilitate access to a system or data.

source code: a series of statements written in a computer programming language that can be converted to computer-executable form.

system vulnerability: a state in a computing system (or set of systems) which either
   ▪ allows an attacker to execute commands as another user

- allows an attacker to access data that is contrary to the specified access restrictions for that data
- allows an attacker to pose as another entity
- allows an attacker to conduct a denial of service [60]

sudo: a program in UNIX, Linux, and similar operating systems such as Mac OS X that allows users to run programs in the guise of another user (normally in the guise of the system's superuser). [61]

---

[60] http://www.cve.mitre.org/about/terminology.html
[61] http://en.wikipedia.org/wiki/Sudo

APPENDIX D: Acknowledgements

The Secret Service and CERT appreciate the work and dedication of the following personnel, without whose efforts this study would not have been possible. With many thanks to the ITS research staff: